

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Masashi Mitomo
Serial No.:
Conf. No.:
Filed: 04/12/2004
For: DEVICE, METHOD AND
PROGRAM FOR
DETECTING
UNAUTHORIZED ACCESS
Art Unit:
Examiner:

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: MS Patent Application, Commissioner for Patents, Alexandria, VA 22313-1450, on this date.

April 12, 2004
Date

Express Mail No. EV 032736202 US

CLAIM FOR PRIORITY

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C., § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2003-368063, filed October 28, 2003

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns
Registration No. 29,367

April 12, 2004
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Facsimile: 312.360.9315

0828, 70177
312.360,0080

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 0 月 2 8 日
Date of Application:

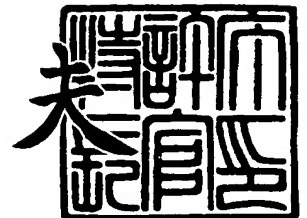
出 願 番 号 特 願 2 0 0 3 - 3 6 8 0 6 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 6 8 0 6 3]

出 願 人 富士通株式会社
Applicant(s):

2 0 0 4 年 2 月 1 9 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 1 1 4 2 1

【書類名】 特許願
【整理番号】 0352432
【提出日】 平成15年10月28日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 11/30
【発明者】
 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社
 内
 【氏名】 三友 仁史
【発明者】
 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社
 内
 【氏名】 東角 芳樹
【発明者】
 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社
 内
 【氏名】 滝澤 文恵
【発明者】
 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社
 内
 【氏名】 鳥居 悟
【発明者】
 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社
 内
 【氏名】 小谷野 修
【特許出願人】
 【識別番号】 000005223
 【氏名又は名称】 富士通株式会社
【代理人】
 【識別番号】 100092152
 【弁理士】
 【氏名又は名称】 服部 毅巖
 【電話番号】 0426-45-6644
【手数料の表示】
 【予納台帳番号】 009874
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9705176

【書類名】 特許請求の範囲**【請求項 1】**

ネットワークを介した不正アクセスを検出するための不正アクセス検知装置において、準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段と、

前記不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する進行中シナリオ記憶手段と、

前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから前記キーデータを抽出するキーデータ抽出手段と、

前記キーデータ抽出手段が抽出した前記キーデータを検索キーとして、前記進行中シナリオ記憶手段から前記進行中シナリオを検索する進行中シナリオ検索手段と、

前記進行中シナリオ検索手段で検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが、前記不正アクセスシナリオ記憶手段に格納されている前記不正アクセスシナリオに沿っているかどうかを照合する照合手段と、

前記照合手段による照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シナリオを更新する進行中シナリオ更新手段と、

前記照合手段による照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力するレポート出力手段と、

を有することを特徴とする不正アクセス検知装置。

【請求項 2】

前記不正アクセスシナリオ記憶手段では、前記不正アクセスシナリオに関し、前記ネットワークを介して行われる処理を示す情報の発信元と宛先とのそれぞれに対して役割が設定されており、

前記照合手段は、前記パケットで示される処理の発信元と宛先とが、前記不正アクセスシナリオで定義された役割を担っているかどうかを判定することを特徴とする請求項 1 記載の不正アクセス検知装置。

【請求項 3】

前記不正アクセスシナリオ記憶手段に格納された前記不正アクセスシナリオは、前記ネットワークを介して行われる処理の指示や応答の際に発生するイベントを契機とした状態遷移によって、準備動作を経て不正アクセスが実行されるまでの処理手順が定義されており、

前記照合手段は、前記パケットで示される処理のイベントによる状態遷移が、前記不正アクセスシナリオに沿っているか否かを判定することを特徴とする請求項 1 記載の不正アクセス検知装置。

【請求項 4】

ネットワークを介した不正アクセスを検出するための不正アクセス検知方法において、

前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから所定のキーデータを抽出し、

準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するための前記キーデータに対応付けて格納する進行中シナリオ記憶手段から、前記パケットから抽出した前記キーデータを検索キーとして前記進行中シナリオを検索し、

前記不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段を参照し、検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが前記不正アクセスシナリオに沿っているかどうかを照合し、

照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シ

ナリオ記憶手段に格納されている前記進行中シナリオを更新し、

照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力する、

ことを特徴とする不正アクセス検知方法。

【請求項 5】

ネットワークを介した不正アクセスを検出するための不正アクセス検知プログラムにおいて、

コンピュータを、

準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段、

前記不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する進行中シナリオ記憶手段、

前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから前記キーデータを抽出するキーデータ抽出手段、

前記キーデータ抽出手段が抽出した前記キーデータを検索キーとして、前記進行中シナリオ記憶手段から前記進行中シナリオを検索する進行中シナリオ検索手段、

前記進行中シナリオ検索手段で検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが、前記不正アクセスシナリオ記憶手段に格納されている前記不正アクセスシナリオに沿っているかどうかを照合する照合手段、

前記照合手段による照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シナリオを更新する進行中シナリオ更新手段、

前記照合手段による照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力するレポート出力手段、

として機能させるための不正アクセス検知プログラム。

【書類名】明細書

【発明の名称】不正アクセス検知装置、不正アクセス検知方法および不正アクセス検知プログラム

【技術分野】

【0001】

本発明はコンピュータへの不正アクセスを検出するための不正アクセス検知装置、不正アクセス検知方法、および不正アクセス検知プログラムに関し、特に攻撃モデルを用いて不正アクセスを検知する不正アクセス検知装置、不正アクセス検知方法、および不正アクセス検知プログラムに関する。

【背景技術】

【0002】

近年の情報通信技術の発展に伴い、インターネットを介したサービスの提供が盛んに行われている。たとえば、サービスの提供者は、インターネットを介してアクセス可能なサーバを設置する。そのサーバにおいて、インターネット経由で接続されたクライアント装置に対して各種サービスを提供する。

【0003】

ただし、サービスを提供するサーバは、インターネットからアクセス可能であるため、不正アクセスによる攻撃の対象になりやすい。そこで、不正アクセスを早期に発見するための技術が必要とされる。

【0004】

基本的には、不正目的のコマンドを含むアクセス要求を検出することで、不正アクセスを発見できる。具体的には、一般に既知のセキュリティホールに対して攻撃を加えるための不正コマンドのリストを予め登録しておく。そして、リストに登録された不正コマンドを含むアクセス要求を検出すると、そのアクセス要求の受付を拒否すると共に、不正アクセスの発生を管理者に通知する。

【0005】

たとえば、脆弱性（セキュリティホール）を有するスクリプトとして“p h f”が良く知られている。“p h f”はウェブサーバ上で動作するスクリプトである。この“p h f”が動作するウェブサーバに対して、不正行為者が所定のH T T P（HyperText Transfer Protocol）リクエストを送信すると、その不正行為者はパスワードファイルを入手することができる。不正行為者が送信する所定H T T Pリクエストには、スクリプトを指定するために“p h f”という文字列が含まれる。そこで、文字列“p h f”を含むH T T Pリクエストを不正アクセスとして検出することができる。

【0006】

ところが、複数の正規なコマンドを組み合わせることで攻撃する不正アクセスも存在する。たとえば、以下のような順序でサーバに値してコマンドを送ることで、不正アクセスが実行されることがある。

【0007】

1. 「ping_sweep」：攻撃者は攻撃の第一歩として、ネットワークツールpingを用いて、動作中のマシンのI P（Internet Protocol）アドレスを取得する。
2. 「Port_scan」：攻撃者は動作中のマシンに対して、各ポートをスキャンする（各T C P（Transmission Control Protocol）ポートが応答するかどうかを検査する処理）。これによって、攻撃者は該当マシンにおいて提供されているサービスの種別を知ることができる。

【0008】

3. 「Fingerprinting」：攻撃者はあるポートに対して適当なパケットを送りつけ、その反応を確かめることによってサーバのソフトウェアの種別・版数等を推定する。
4. 「Hijacking」：サーバで動作するソフトウェアの種別・版数に応じた脆弱性が分かたした場合、攻撃者は脆弱性を利用してマシンを乗っ取る（任意のプログラムを該当マシンに実行させることができるようにすること）。

【0009】

5. 「Deploy_Back_door」: 攻撃者は、乗っ取ったマシンにバックドアプログラムを導入する。バックドアプログラムは、攻撃者による該当マシンの自由な操作を容易にするためのツールである。

【0010】

このような場合、個々のアクセス要求に含まれるコマンドだけでは、不正を検出することができない。そこで、攻撃の準備行為を状態遷移で表した攻撃モデルを登録しておく。そして、イベントそれぞれを関連付けて手順として検出し、攻撃モデルと比較することで不正アクセスを検知することができる（たとえば、非特許文献1参照）。

【非特許文献1】三友仁史 他、「攻撃モデルを用いたDDoS攻撃の予兆検知方式」、情報処理学会 第65回全国大会、2003年3月、第65回情報処理学会全国大会公演論文集 第三分冊 p. 207-208

【発明の開示】

【発明が解決しようとする課題】

【0011】

しかし、従来の方式では、大量のイベントが発生するサーバ上では、処理負荷が過大になってしまうという問題がある。すなわち、従来の方式では、リアルタイムに入力されるイベントシーケンスに対し、保持している「それまでのイベント履歴」と攻撃モデルとを照合することで不正アクセスの検知を行う。この場合、イベントが1つ入力されるごとに、全てのイベント履歴を追跡し、攻撃モデル中のイベント遷移が出現するかを判定する必要がある。そのため、長期間の運用によってイベント履歴が膨大になった場合、不正アクセスの検知がリアルタイムに行えない恐れがある。

【0012】

本発明はこのような点に鑑みてなされたものであり、一連の準備段階の処理を経て実行される不正アクセスをリアルタイムに検知することができる不正アクセス検知装置、不正アクセス検知方法、および不正アクセス検知プログラムを提供することを目的とする。

【課題を解決するための手段】

【0013】

本発明では上記課題を解決するために、図1に示すような不正アクセス検知装置1が提供される。本発明に係る不正アクセス検知装置1は、ネットワーク2を介した不正アクセスを検出するためのものである。この不正アクセス検知装置1は、以下の要素で構成される。

【0014】

不正アクセスシナリオ記憶手段1aは、準備動作を経て不正アクセスが実行されるまでにネットワーク2を介して行われる処理の手順を定義した不正アクセスシナリオが格納されている。進行中シナリオ記憶手段1bは、不正アクセスシナリオに沿ってネットワーク2を介して行われた処理の経過を示す進行中シナリオを、進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する。キーデータ抽出手段1cは、ネットワーク2を介して通信されるパケット5を取得し、取得したパケット5からキーデータを抽出する。進行中シナリオ検索手段1dは、キーデータ抽出手段1cが抽出したキーデータを検索キーとして、進行中シナリオ記憶手段1bから進行中シナリオを検索する。照合手段1eは、進行中シナリオ検索手段1dで検出された進行中シナリオに続けてパケット5で示される処理を行うことが、不正アクセスシナリオ記憶手段1aに格納されている不正アクセスシナリオに沿っているかどうかを照合する。進行中シナリオ更新手段1fは、照合手段1eによる照合の結果、不正アクセスシナリオに沿っていると判断されたとき、進行中シナリオ記憶手段1bに格納されている進行中シナリオを更新する。レポート出力手段1gは、照合手段1eによる照合の結果に基づいて、不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポート6を出力する。

【0015】

このような不正アクセス検知装置によれば、パケット5がネットワーク2上で通信され

ると、そのパケット5がキーデータ抽出手段1cで取得され、キーデータが抽出される。次に、進行中シナリオ検索手段1dにより、キーデータ抽出手段1cが抽出したキーデータを検索キーとして、進行中シナリオ記憶手段1bから進行中シナリオが検索される。さらに、照合手段1eにより、進行中シナリオ検索手段1dで検出された進行中シナリオに続けてパケット5で示される処理を行うことが、不正アクセスシナリオ記憶手段1aに格納されている不正アクセスシナリオに沿っているかどうか照合される。照合手段1eによる照合の結果、不正アクセスシナリオに沿っていると判断されたとき、進行中シナリオ更新手段1fにより、進行中シナリオ記憶手段1bに格納されている進行中シナリオが更新される。また、レポート出力手段1gにより、照合手段1eによる照合の結果に基づいて、不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポート6が出力される。

【0016】

また、本発明では上記課題を解決するために、ネットワークを介した不正アクセスを検出するための不正アクセス検知方法において、前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから所定のキーデータを抽出し、準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する進行中シナリオ記憶手段から、前記パケットから抽出した前記キーデータを検索キーとして前記進行中シナリオを検索し、前記不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段を参照し、検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが前記不正アクセスシナリオに沿っているかどうかを照合し、照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シナリオを更新し、照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力する、ことを特徴とする不正アクセス検知方法が提供される。

【0017】

このような不正アクセス検知方法によれば、パケットがネットワーク上で通信されると、そのパケットからキーデータが抽出される。次に、抽出したキーデータを検索キーとして、進行中シナリオ記憶手段から進行中シナリオが検索される。さらに、検出された進行中シナリオに続けてパケットで示される処理を行うことが、不正アクセスシナリオ記憶手段に格納されている不正アクセスシナリオに沿っているかどうか照合される。照合の結果、不正アクセスシナリオに沿っていると判断されたとき、進行中シナリオ記憶手段に格納されている進行中シナリオが更新される。また、照合の結果に基づいて、不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートが出力される。

【0018】

また、上記課題を解決するために、ネットワークを介した不正アクセスを検出するための不正アクセス検知プログラムにおいて、コンピュータを、準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段、前記不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する進行中シナリオ記憶手段、前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから前記キーデータを抽出するキーデータ抽出手段、キーデータ抽出手段が抽出した前記キーデータを検索キーとして、前記進行中シナリオ記憶手段から前記進行中シナリオを検索する進行中シナリオ検索手段、前記進行中シナリオ検索手段で検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが、前記不正アクセスシナリオ記憶手段に格納されている前記不正アクセスシナリオに沿っているかどうかを照合する照合手段、前記照合手段による照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シ

ナリオを更新する進行中シナリオ更新手段、前記照合手段による照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力するレポート出力手段、として機能させるための不正アクセス検知プログラムが提供される。

【0019】

このような不正アクセス検知プログラムをコンピュータに実行させることで、コンピュータが上記不正アクセス検知装置として機能する。

【発明の効果】

【0020】

以上説明したように本発明では、キーデータを検索キーとして進行中シナリオを検索し、検出された進行中シナリオに続けてパケットで示される処理を行うことと、不正アクセスシナリオとの照合を行うようにした。そのため、格納されている全ての進行中シナリオの照合を行う必要が無くなり、一連の準備段階の処理を経て実行される不正アクセスをリアルタイムに検知することが可能となる。

【発明を実施するための最良の形態】

【0021】

以下、本発明の実施の形態を図面を参照して説明する。

まず、実施の形態に適用される発明の概要について説明し、その後、実施の形態の具体的な内容を説明する。

【0022】

図1は、実施の形態に適用される発明の概念図である。不正アクセス検知装置1は、ネットワーク2を介した不正アクセスを検出するためのものである。図1に示すように、不正アクセス検知装置1は、不正アクセスシナリオ記憶手段1a、進行中シナリオ記憶手段1b、キーデータ抽出手段1c、進行中シナリオ検索手段1d、照合手段1e、進行中シナリオ更新手段1f、およびレポート出力手段1gを有している。

【0023】

不正アクセスシナリオ記憶手段1aには、不正アクセスシナリオが格納されている。不正アクセスシナリオは、準備動作を経て不正アクセスが実行されるまでにネットワーク2を介して行われる処理の手順を定義したものである。たとえば、不正アクセスシナリオは、ネットワーク2を介して行われる処理の指示や応答の際に発生するイベントの遷移によって、準備動作を経て不正アクセスが実行されるまでの処理手順を定義することができる。

【0024】

進行中シナリオ記憶手段1bは、不正アクセスシナリオに沿ってネットワーク2を介して行われた処理の経過を示す進行中シナリオを、進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する。キーデータは、たとえば、パケット5の発信元アドレスと宛先アドレスとである。

【0025】

キーデータ抽出手段1cは、ネットワーク2を介して通信されるパケット5を取得し、取得したパケット5からキーデータを抽出する。たとえば、発信元装置3から宛先装置4に対して送信されたパケット5から、発信元装置3のアドレスと宛先装置4のアドレスとが抽出される。

【0026】

進行中シナリオ検索手段1dは、キーデータ抽出手段1cが抽出したキーデータを検索キーとして、進行中シナリオ記憶手段1bから進行中シナリオを検索する。たとえば、発信元装置3のアドレスと宛先装置4のアドレスとの両方を含む進行中シナリオが検索される。

【0027】

照合手段1eは、進行中シナリオ検索手段1dで検出された進行中シナリオに続けてパケット5で示される処理を行うことが、不正アクセスシナリオ記憶手段1aに格納されて

いる不正アクセスシナリオに沿っているかどうかを照合する。

【0028】

進行中シナリオ更新手段1 fは、照合手段1 eによる照合の結果、不正アクセスシナリオに沿っていると判断されたとき、進行中シナリオ記憶手段1 bに格納されている進行中シナリオを更新する。

【0029】

レポート出力手段1 gは、照合手段1 eによる照合の結果に基づいて、不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポート6を出力する。たとえば、レポート出力手段1 gは、進行中シナリオ検索手段1 dで検出された進行中シナリオが、不正アクセスシナリオの最後の処理まで進行したときに不正アクセスレポート6を出力する。

【0030】

このような不正アクセス検知装置によれば、パケット5がネットワーク2上で通信されると、そのパケット5がキーデータ抽出手段1 cで取得され、キーデータが抽出される。次に、進行中シナリオ検索手段1 dにより、キーデータ抽出手段1 cが抽出したキーデータを検索キーとして、進行中シナリオ記憶手段1 bから進行中シナリオが検索される。さらに、照合手段1 eにより、進行中シナリオ検索手段1 dで検出された進行中シナリオに続けてパケット5で示される処理を行うことが、不正アクセスシナリオ記憶手段1 aに格納されている不正アクセスシナリオに沿っているかどうかを照合される。照合手段1 eによる照合の結果、不正アクセスシナリオに沿っていると判断されたとき、進行中シナリオ更新手段1 fにより、進行中シナリオ記憶手段1 bに格納されている進行中シナリオが更新される。また、レポート出力手段1 gにより、照合手段1 eによる照合の結果に基づいて、不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポート6が出力される。

【0031】

このように、本発明では、イベント履歴を保持する代わりに、進行中シナリオを、あるキーデータをキーとしてデータベース化して保持することにした。ここで、キーデータは、不正アクセスシナリオ記憶手段1 a中で定義された不正アクセスシナリオにおいて、シナリオを構成する各イベントに対して共通に関連付けられているべき情報である（たとえば、発信元アドレスや宛先アドレス）。

【0032】

これにより、リアルタイムに入力されるパケットから抽出されるキーデータに基づき、それらが関連する進行中シナリオをリアルタイムに特定できる。また、不正アクセスシナリオ記憶手段1 a中の不正アクセスシナリオとの照合も、キーデータにより検出された進行中シナリオに関してのみ行えばよい。そのため、処理時間が短くて済む。その結果、不正アクセスの検知がリアルタイムに行える。

【0033】

なお、進行中シナリオ記憶手段1 bにおいて、進行中シナリオに対応付けて、進行中シナリオの進捗度を示す数値を記憶させることもできる。この場合、進行中シナリオ更新手段1 fは、進捗度の数値を増加させることで、進行中シナリオを更新する。

【0034】

また、レポート出力手段1 gは、進捗度が所定の値を超えたとき、不正アクセスレポートを出力するようにすることができる。すなわち、不正アクセスシナリオの最終段階まで進行中シナリオが進んでいなくても、進捗度が有る程度以上進んだ場合、不正アクセスレポート6が出力される。これにより、不正アクセスの予兆が現れたときに不正アクセスレポートを出力できる。

【0035】

さらに、不正アクセスシナリオ記憶手段1 aでは、不正アクセスシナリオに関し、ネットワーク2を介して行われる処理を示す情報（たとえばパケット）の発信元と宛先とのそれぞれに対して役割を設定することができる。この場合、照合手段1 eは、パケットで示

される処理の発信元と宛先とが、不正アクセスシナリオで定義された役割を担っているかどうかを判定する。すなわち、役割に沿った処理を示すパケットを取得した場合にのみ、進行中シナリオが進行するものと判断される。これにより、役割の異なる3台以上の装置が関係する不正アクセスの検知が可能となる。

【0036】

また、不正アクセスシナリオは、ネットワーク2を介して行われる処理の指示や応答の際に発生するイベントを契機とした状態遷移によって、準備動作を経て不正アクセスが実行されるまでの処理手順を定義することができる。この場合、照合手段1eは、パケット5で示される処理のイベントによる状態遷移が、不正アクセスシナリオに沿っているか否かを判定する。これにより、攻撃の実行までに複数のイベントが複雑に関係し合っている場合であっても、不正アクセスの準備状態の進捗を把握することができる。

【0037】

また、不正アクセスシナリオには、処理が次の段階へ進行するまでの有効期限を設定することもできる。この場合、照合手段1eは、パケットで示される処理が、有効期限内に発生した処理かどうかを判定する。すなわち、有効期限内に次の段階の処理が発生した場合にのみ、進行中シナリオが進行するものと判断される。これにより、途中で処理の進行が中止された進行中シナリオに基づいて、誤って不正アクセスレポートを出力する事態を防止することができる。

【0038】

このとき、進行中シナリオ更新手段1fは、有効期限の切れた進行中シナリオを進行中シナリオ記憶手段1bから削除することができる。これにより、途中で停止した不要な進行中シナリオを効率よく削除できる。

【0039】

また、不正アクセスシナリオは、シナリオが進行する毎に加算される重みを定義することができる。この場合、レポート出力手段1gは、重みのトータルが所定値を超えたとき、不正アクセスレポート6を出力する。これにより、不正アクセスが実行される危険性が高くなったときに攻撃の予兆を検知し、実際の攻撃前に不正アクセスレポート6を出力することができる。

【0040】

また、照合手段1eは、将来起こりうる不正シナリオにおける被害の種類、大きさ、期間等について予測することもできる。予測内容に応じた対策を施すことで、不正アクセスの内容に応じた適切な対応が可能となる。

【0041】

さらに必要に応じて、不正シナリオに関わる装置、ネットワーク2などに関する情報を、ネットワーク2越しに取得、解析することで、将来起こりうる不正シナリオにおける被害を予測することも可能である。

【0042】

以下に本発明の実施の形態を具体的に説明する。

【第1の実施の形態】

まず、第1の実施の形態について説明する。

【0043】

図2は、第1の実施の形態に係るネットワークシステムの構成例を示す図である。図2に示すように、イントラネット21とインターネット22との間にファイアウォール(FW)200が設置されている。ファイアウォール200はネットワーク10に接続されている。

【0044】

ネットワーク10は、インターネット22に接続されたクライアント31, 32, 33, ... からアクセス可能なネットワークである。ネットワーク10には、不正アクセス検知装置100、ウェブサーバ210、メールサーバ220などが接続されている。ウェブサーバ210は、インターネット22を介してウェブページ等のコンテンツの提供サー

ビスを行うサーバコンピュータである。メールサーバ220は、イントラネット21とインターネット22とを介した電子メール送受信サービスを行うサーバコンピュータである。

【0045】

不正アクセス検知装置100は、IDS（侵入検知システム）等の機能を利用してネットワーク10上の装置へのインターネット22を介した不正アクセスを監視するコンピュータである。すなわち、ウェブサーバ210やメールサーバ220は、所定のサービスをインターネット22を介して提供するため、IPアドレスが公開されている。そのため、ウェブサーバ210やメールサーバ220は、不正進入等の攻撃を受けやすい。そこで、不正アクセス検知装置100は、ネットワーク10を介して伝送されるパケットを監視し、ウェブサーバ210やメールサーバ220に対する不正アクセスを検出する。

【0046】

図3は、本発明の実施の形態に用いる不正アクセス検知装置のハードウェア構成例を示す図である。不正アクセス検知装置100は、CPU（Central Processing Unit）101によって装置全体が制御されている。CPU101には、バス107を介してRAM（Random Access Memory）102、ハードディスクドライブ（HDD:Hard Disk Drive）103、グラフィック処理装置104、入力インタフェース105、および通信インタフェース106が接続されている。

【0047】

RAM102には、CPU101に実行させるOS（Operating System）のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、RAM102には、CPU101による処理に必要な各種データが格納される。HDD103には、OSやアプリケーションプログラムが格納される。

【0048】

グラフィック処理装置104には、モニタ11が接続されている。グラフィック処理装置104は、CPU101からの命令に従って、画像をモニタ11の画面に表示させる。入力インタフェース105には、キーボード12とマウス13とが接続されている。入力インタフェース105は、キーボード12やマウス13から送られてくる信号を、バス107を介してCPU101に送信する。

【0049】

通信インタフェース106は、ネットワーク10に接続されている。通信インタフェース106は、ネットワーク10を介して、他のコンピュータとの間でデータの送受信を行う。

【0050】

以上のようなハードウェア構成によって、第1の実施の形態の処理機能を実現することができる。なお、図3には、不正アクセス検知装置100のハードウェア構成を示したが、ファイアウォール200、ウェブサーバ210、メールサーバ220、およびクライアント31、32、33、・・・も同様のハードウェア構成で実現することができる。

【0051】

図4は、第1の実施の形態に係る不正アクセス検知装置の内部構成を示すブロック図である。不正アクセス検知装置100は、通信処理部110、パケットモニタ部120、シナリオ検出部130、および攻撃レポート部140を有している。

【0052】

通信処理部110は、ネットワーク10を介した通信を行う。この通信処理部110は、不正アクセス検知装置100宛のパケットに限らず、ウェブサーバ210やメールサーバ220宛のパケットも取り込み、パケットモニタ部120へ渡す。

【0053】

パケットモニタ部120は、ネットワーク10を介して伝送されるパケットを解析し、そのパケットに基づくイベントを検出する。パケットモニタ部120は、検出したイベントをシナリオ検出部130に渡す。

【0054】

シナリオ検出部130は、パケットモニタ部120で検出されたイベントに基づいて、不正アクセスシナリオに沿ったイベント遷移を検出する。そして、検出されたイベント遷移を不正アクセスレポートとして攻撃レポート部140に通知する。

【0055】

攻撃レポート部140は、シナリオ検出部130から検出されたイベント遷移を元に将来の攻撃予測に関する攻撃レポート41、42、43、・・・を生成し、管理者に対して通知する。攻撃レポート41、42、43、・・・の通知方法として、たとえば、管理者が使用している端末装置の画面にレポートの内容を表示させることができる。また、即時対応が不要な内容のレポートであれば、管理者に対して電子メールにより攻撃レポート41、42、43、・・・を通知することもできる。

【0056】

このような構成により、ネットワーク10を介した通信のパケットが通信処理部110で取得され、パケットモニタ部120でイベントが検出される。検出されたイベントはシナリオ検出部130に渡され、不正アクセスシナリオと照合される。不正アクセスシナリオに沿ったイベント遷移が検出されると、その内容が攻撃レポート部140に通知され、攻撃レポート41、42、43、・・・が出力される。

【0057】

次に、シナリオ検出部130の詳細について説明する。

図5は、第1の実施の形態のシナリオ検出部の機能を示すブロック図である。シナリオ検出部130は、シナリオ定義データベース(DB)131、進行中シナリオDB132、関連ホスト抽出部133、進行中シナリオ検索部134、イベント系列照合部135、進行中シナリオ更新部136、および検出シナリオ出力部137を有している。

【0058】

図5において、イベント51、52、53、・・・は、ネットワーク10上でパケットモニタ部120によって、リアルタイムに検出されたイベントである。このようなイベント51、52、53、・・・には、その名称(イベントの名前)、発信元IPアドレス、宛先IPアドレス、検出時刻などが情報として含まれている。

【0059】

また、第1の実施の形態においては、イベントに関連付けるキーデータは「発信元IPアドレス」「宛先IPアドレス」となる。なお、時刻をキーデータとすることもできる。

シナリオ定義DB131は、予め定義された不正アクセスシナリオが格納されたデータベースである。不正アクセスは所定のシナリオに沿って進行することが多いため、シナリオ定義DB131には、不正アクセスシナリオがイベント遷移で表現されている。

【0060】

進行中シナリオDB132は、キーデータによって関連付けられるイベントの遷移(進行中イベント)が登録されたデータベースである。進行中シナリオDB132には、発信元IPアドレス、宛先IPアドレス、対応する不正アクセスイベントの名前、進捗度等が進行中のシナリオ毎に登録されている。

【0061】

関連ホスト抽出部133は、リアルタイムに入力されるイベント51、52、53、・・・からキーデータとして、「発信元IPアドレス」と「宛先IPアドレス」とを抽出する。

【0062】

進行中シナリオ検索部134は、関連ホスト抽出部133が抽出した「発信元IPアドレス」と「宛先IPアドレス」とを検索キーとして、進行中シナリオDB132を検索する。検出された進行中シナリオは、イベント系列照合部135に渡される。

【0063】

イベント系列照合部135は、進行中シナリオ検索部134により進行中シナリオDB132からエントリが検出された場合、そのエントリが保持している「不正アクセスイベ

ントの名前」「進捗度」を取得する。そして、イベント系列照合部135は、シナリオ定義DB131を参照し、入力されたイベントの名称に基づき、検出された進行中シナリオから入力されたイベントへの遷移が不正アクセスシナリオに沿っているかどうかを判定する。不正アクセスシナリオに沿ったイベントが発生していれば、その旨が進行中シナリオ更新部136に通知される。

【0064】

また、イベント系列照合部135は、シナリオ定義DB131を参照し、入力されたイベントが先頭となるイベント遷移が有る場合、そのイベント遷移が開始されたことを進行中シナリオ更新部136に通知する。さらに、イベント系列照合部135は、進行中シナリオのイベント遷移が不正アクセスシナリオの終端まで達したとき、進行中シナリオの情報を検出シナリオ出力部137に渡す。

【0065】

進行中シナリオ更新部136は、イベント系列照合部135からシナリオに沿ったイベント発生の通知を受けて、進行中シナリオDB132における該当エントリの「進捗度」を更新する。

【0066】

また、進行中シナリオ更新部136は、シナリオ定義DB131中のエントリにおいて先頭イベントが現在処理中のイベントと同じ場合、これに該当するエントリを進行中シナリオDB132に追加する。

【0067】

検出シナリオ出力部137は、イベント系列照合部135においてイベント遷移が不正アクセスシナリオの終端まで達したと判断されたとき、不正なアクセスを検出したとして、外部に不正アクセスレポート61, 62, 63, ...を出力する。不正アクセスレポート61, 62, 63, ...には、検出された進行中シナリオに関する情報（発信元IPアドレスや宛先IPアドレスなど）が含まれる。

【0068】

図6は、シナリオ定義DBのデータ構造例を示す図である。シナリオ定義DB131には、不正アクセスシナリオ名に対応付けて、不正アクセスが行われるときのイベント遷移が登録されている。イベント遷移は、イベント名の配列で表されている。

【0069】

たとえば、不正アクセスシナリオAは、最初にイベントaが発生し、次にイベントbが発生し、最後にイベントc発生するというシナリオを表している。また、不正アクセスシナリオBは、最初にイベントaが発生し、次にイベントdが発生し、次にイベントe発生し、最後にイベント遷移cが発生するというシナリオを表している。

【0070】

シナリオ定義DB131に定義された不正アクセスシナリオに沿って、キーデータで関連付けられたイベント遷移が発生した場合、不正アクセスが検出されたことになる。

図7は、進行中シナリオDBのデータ構造例を示す図である。進行中シナリオDB132は、発信元IPアドレスと宛先IPアドレスとの組、不正アクセスシナリオ名、進捗度が互いに関連付けられ、1つのエントリとして登録されている。

【0071】

各エントリは、装置間の通信における進行中シナリオの進行状況を示している。すなわち、進行中シナリオの「発信元IPアドレス」「宛先IPアドレス」をキーデータ（検索対象項目）として、そのキーデータに対応付けて、不正アクセスシナリオ名や、その進捗度を保持している。進捗度は、現在イベント遷移の何番目まで進行しているのかによって、シナリオの進行状態を示している。

【0072】

たとえば、発信元IPアドレス「192.168.1.5」の装置と宛先IPアドレス「10.10.100.100」の装置との間では、不正アクセスシナリオBに沿った進行中シナリオが、2番目のイベントまで進行している。また、発信元IPアドレス「10.1.1.123」の装置と宛先IP

アドレス「192.168.30.30」の装置との間では、不正アクセスシナリオDに沿った進行中シナリオが、3番目のイベントまで進行している。

【0073】

以上のような構成のシナリオ検出部130において、以下のようなシナリオ検出処理が行われる。

図8は、シナリオ検出処理の手順を示すフローチャートである。以下、図8に示す処理をステップ番号に沿って説明する。

【0074】

【ステップS11】関連ホスト抽出部133は、イベントの入力を受け付けると、処理をステップS12に進める。

【ステップS12】関連ホスト抽出部133は、入力されたイベントからキーデータを抽出する。第1の実施の形態では、キーデータとして発信元IPアドレスと宛先IPアドレスとが抽出される。抽出されたキーデータは、進行中シナリオ検索部134に渡される。

【0075】

【ステップS13】進行中シナリオ検索部134は、関連ホスト抽出部133から抽出された発信元IPアドレスと宛先IPアドレスとを検索キーとして、進行中シナリオDB132から進行中シナリオのエントリを検索する（2つの検索キーの論理積（AND）を検索条件とする）。そして、進行中シナリオ検索部134は、検索結果として得られた進行中シナリオをリストアップする。リストアップされた進行中シナリオは、イベント系列照合部135に渡される。

【0076】

たとえばイベント51が入力され、そのイベント51の発信元IPアドレスが「192.168.1.5」、宛先IPアドレスが「10.10.100.100」、イベント名が「e」であった場合を考える。このとき、進行中シナリオDB132の内容が図7の通りであれば、イベント51の発信元IPアドレス及び宛先IPアドレスから、進行中シナリオDB132内の第一エントリが検出される。

【0077】

【ステップS14】イベント系列照合部135は、進行中シナリオ検索部134によってリストアップされている進行中シナリオがあるか否かを判断する。進行中シナリオがある場合、処理がステップS15に進められる。進行中シナリオが無い場合、処理がステップS22に進められる。

【0078】

【ステップS15】イベント系列照合部135は、リストアップされた1つの進行中シナリオに対し、入力されたイベントによる進行の有無を判定する。

具体的には、イベント系列照合部135は、シナリオ定義DB131を参照し、ステップS13で検出された進行中シナリオから入力されたイベントへの遷移と、予め定義されている不正アクセスシナリオとを照合する。次に、イベント系列照合部135は、検出された進行中シナリオのイベント遷移が、ステップS11で入力されたイベントへ遷移したときに、不正アクセスシナリオ名で特定される不正アクセスシナリオに沿っているか否かを判断する。イベント遷移（イベント名の配列）が前方一致すれば、不正アクセスシナリオに沿っていると判断される。不正アクセスシナリオに沿ったイベント遷移であれば、イベント系列照合部135は、シナリオが進行すると判定する。

【0079】

たとえば、ステップS13の説明で示したようなイベント51が入力された場合、シナリオは「不正アクセスシナリオB」において「2番目」まで進行していることが分かる。そこでシナリオ定義DB131で「不正アクセスシナリオB」を参照すると、イベント名「e」が入力された場合に次の遷移が発生する（すなわち、「状態」が変化する）ことがわかる。ステップS11で入力されたイベント51の名前は「e」であるため、不正アクセスシナリオに沿ったイベント遷移が発生し、シナリオが進行する。

【0080】

また、シナリオ定義DB131に定義されている不正アクセスシナリオにおける先頭のイベントに対応するイベントが入力された場合、新規のシナリオのイベント遷移が発生したものと判断される。

【0081】

〔ステップS16〕 イベント系列照合部135は、照合の結果、イベント遷移が発生し、進行中シナリオが進行するか否かを判断する。進行中シナリオが進行する場合、処理がステップS17に進められる。進行中シナリオが進行しない場合、処理がステップS21に進められる。

【0082】

〔ステップS17〕 進行中シナリオ更新部136は、イベント遷移が発生した進行中シナリオのエントリを更新する。具体的には、進行中シナリオ更新部136は、該当する進行中シナリオの進捗度を1段階進める。

【0083】

たとえば、ステップS13の説明で示したようなイベント51が入力された場合、進行中シナリオDB132の第一エントリの「進捗度」が「2番目」から「3番目」に更新される。

【0084】

〔ステップS18〕 イベント系列照合部135は、不正アクセスレポートの出力の要否を判定する。たとえば、イベント系列照合部135は、ステップS17で進行させた進行中シナリオが、シナリオ定義DB131に定義された不正アクセスシナリオの終端に達した場合、不正アクセスレポートの出力が必要であると判断する。

【0085】

〔ステップS19〕 イベント系列照合部135は、不正アクセスレポートの出力が必要な場合、不正アクセスが発生したことを検出シナリオ出力部137に通知し、処理をステップS20に進める。不正アクセスレポートの出力が不要な場合、処理をステップS21に進める。

【0086】

〔ステップS20〕 検出シナリオ出力部137は、イベント系列照合部135から通知された内容に応じた不正アクセスレポートを生成し、出力する。

〔ステップS21〕 イベント系列照合部135は、処理対象となっている進行中シナリオを、ステップS13で生成されたリストから削除する。その後、処理がステップS14に進められ、リストアップされている他の進行中シナリオに対して、ステップS14～ステップS20の処理が行われる。

【0087】

〔ステップS22〕 リストアップされている進行中シナリオが無くなったとき、進行中シナリオ更新部136は、入力されたイベントによって開始する新たな進行中シナリオを、進行中シナリオDB132に追加する。すなわち、進行中シナリオ更新部136は、シナリオ定義DB131中の不正アクセスシナリオにおいて先頭イベントがステップS11で入力されたイベントと同じ場合、これに該当するエントリ（新規の進行中シナリオ）を進行中シナリオDB132に追加する。

【0088】

たとえば、ステップS13の説明で示したようなイベント51が入力された場合、シナリオ定義DB131において先頭イベントが「イベントe」の不正アクセスシナリオそれぞれに対応付けて、進捗度を「1番目」としたエントリが進行中シナリオDB132に追加される。その後、処理が終了する。

【0089】

このようにして、第1のコンピュータから第2のコンピュータに対して、不正アクセスシナリオに沿ったイベントを含むパケットが送信された場合、不正アクセスを検出して、管理者に通知することができる。この場合、不正アクセスレポートには、攻撃者が使用する

る装置のIPアドレス、攻撃を受けている装置のIPアドレス、完了した不正アクセスシナリオの名前等が含まれる。

【0090】

このように第1の実施の形態では、キーデータが一致する進行中シナリオのイベント遷移のみを調査するため、不正アクセスシナリオとの照合処理が非常に簡単である。その結果、インターネット22等の大規模なネットワークを介して大量のパケットがネットワーク10上で送受信されても、リアルタイムに不正アクセスを検出することができる。

【0091】

特に、不正アクセスには、サーバの負荷を過大にすることでセキュリティホールを発生させる攻撃もある。そのため、トラフィックが混雑している状態でも安定して不正アクセスを検出できることは、システムの安全性を確保する上で重要である。

【0092】

〔第2の実施の形態〕

次に、第2の実施の形態について説明する。第2の実施の形態は、イベントの発信元や宛先が変遷するような不正アクセスを検知できるようにしたものである。イベントの発信元や宛先が変遷するような不正アクセスとしては、たとえば、DDoS (Distributed Denial of Service: 分散型サービス不能化) 攻撃がある。

【0093】

DDoS攻撃とは、複数の踏み台（ネットワークを介して悪者に乗っ取られた装置）から1つのターゲットに向けて一斉に大量のパケットを送りつける攻撃である。DDoS攻撃は専用のツール（DDoS攻撃発生ツール）を用いて行われることが多く、それには様々な種類がある。

【0094】

図9は、DDoS攻撃の発生メカニズムを示す概念図である。図9の例では、クライアント31を利用して、ウェブサーバ210に攻撃を加える場合を想定している。

クライアント31を使用する攻撃者は、インターネット22からアクセス可能なコンピュータをエージェント241, 242, 243, ...として機能させる。クライアント31から各エージェント241, 242, 243, ...へは、ハンドラ230を経由して指示を送る。

【0095】

ここで、「エージェント」とは、DDoS攻撃の目標（任意の装置あるいはネットワーク）に向けて大量のパケットを送りつける処理機能である。すなわち、「エージェント」はターゲットに直接被害を及ぼすホストとなる。

【0096】

また、「ハンドラ」とは、攻撃者の使用するクライアント31とエージェント241, 242, 243, ...とのインタフェースに相当し、攻撃者がエージェントを操作するための機能である。「ハンドラ」とはエージェントに対して外部から指令を出すホストとなる。

【0097】

エージェント241, 242, 243, ...やハンドラ230は、一般にネットワーク越しに攻撃者によって乗っ取られた脆弱なマシンにインストールされる。

攻撃者はクライアント31を操作し、ハンドラ230にコマンドを与える。ハンドラ230は、コマンドが与えられると、それをエージェント241, 242, 243, ...に対する操作・設定コマンドに変換し、各エージェント241, 242, 243, ...に送信する。エージェント241, 242, 243, ...は一種のサーバソフトウェアによる処理機能であり、ハンドラ230からコマンドを受信すると、その内容に応じた攻撃を実行する。たとえば、攻撃対象のウェブサーバ210に対して、大量のパケットを送信する（パケットフラッド）。

【0098】

これらハンドラ230やエージェント241, 242, 243, ...をネットワーク

上のコンピュータに導入するためのソフトウェアのインストール及び設定は、ネットワークを介して行われる。よって、これらに係る通信は（暗号化されていない限り）ネットワーク上で検出可能である。

【0099】

そこで、第2の実施の形態では、攻撃者がハンドラ230とするコンピュータの乗っ取りや、エージェント241, 242, 243, ...へのコマンドの送信等の攻撃のシナリオを不正アクセス検知装置300に登録する。不正アクセス検知装置300は、予め登録された不正アクセスシナリオに沿ったイベント遷移を監視する。そして、不正アクセスシナリオに沿ったイベント遷移が攻撃の準備段階まで進んだとき、不正アクセス検知装置300は、ウェブサーバ210の管理者や、ハンドラ230やエージェント241, 242, 243, ...の管理者へ、不正アクセスの発生の予告通知を行う。

【0100】

なお、DDoS攻撃では、不正アクセスに関与する装置が多数あるため、2つのコンピュータ間の通信（1台が発信元、他の1台が宛先）のイベント遷移だけを監視したのでは、DDoS攻撃を検出できない。そこで、第2の実施の形態に係る不正アクセス検知装置300では、不正アクセスシナリオにおいて、各装置の役割に応じたイベント遷移を定義する。

【0101】

さらに、不正アクセス検知装置300は、進行中シナリオを記憶するとき、検出したイベントに関与する装置に、不正アクセスシナリオ上の役割を設定する。そして、役割が設定された各装置間で、各役割に従って不正アクセスシナリオに沿ったイベント遷移が行われたとき、不正アクセス検知装置300において不正アクセスの検出が行われる。

【0102】

なお、図9に示す不正アクセス検知装置300、ハンドラ230、エージェント241, 242, 243, ...のハードウェア構成は、図3に示した構成と同様である。

以下、第2の実施の形態に係る不正アクセス検知装置300の機能について詳細に説明する。

【0103】

図10は、第2の実施の形態に係る不正アクセス検知装置の内部構成を示すブロック図である。不正アクセス検知装置300は、通信処理部310、パケットモニタ部320、シナリオ検出部330、引数抽出部340、および攻撃レポート部350を有している。

【0104】

通信処理部310は、図4に示した第1の実施の形態の通信処理部110と同様の機能を有している。パケットモニタ部320は、図4に示した第1の実施の形態のパケットモニタ部120と同様の機能を有している。ただし、パケットモニタ部320は、検出したイベントを、シナリオ検出部330だけでなく引数抽出部340にも渡す。

【0105】

シナリオ検出部330は、パケットモニタ部320で検出されたイベントに基づいて、不正アクセスシナリオに沿ったイベント遷移を検出する。そして、不正アクセスシナリオに沿ったイベント遷移に基づいて不正アクセスレポートの出力を行う。シナリオ検出部330は、不正アクセスレポートを攻撃レポート部350に通知する。

【0106】

引数抽出部340は、パケットモニタ部320から受け取ったイベントから、DDoS攻撃におけるハンドラ230からエージェント241, 242, 243, ...への設定コマンドの引数を抽出する。抽出した引数は攻撃レポート部350に渡され、攻撃レポート71, 72, 73, ...に反映される。

【0107】

攻撃レポート部350は、シナリオ検出部330から検出されたイベント遷移を元に将来の攻撃に関する攻撃レポート71, 72, 73, ...を生成し、処理のコンピュータ（ハンドラ230やエージェント241, 242, 243, ...）の管理者に対して通

知する。攻撃レポート 71, 72, 73, . . . の通知方法として、たとえば、管理者が使用している端末装置の画面にレポートの内容を表示させることができる。また、即時対応が不要な内容のレポートであれば、電子メール等により攻撃レポート 71, 72, 73, . . . を通知することもできる。

【0108】

このような構成の不正アクセス検知装置 300 のシナリオ検出部 330 において、DDoS 攻撃の発生が検出される。

図 11 は、第 2 の実施の形態のシナリオ検出部の機能を示すブロック図である。シナリオ検出部 330 は、役割指定シナリオ定義データベース (DB) 331、役割指定進行中シナリオ DB 332、関連ホスト抽出部 333、役割指定進行中シナリオ検索部 334、イベント系列照合部 335、役割指定進行中シナリオ更新部 336、および検出シナリオ出力部 337 を有している。

【0109】

関連ホスト抽出部 333、イベント系列照合部 335、および検出シナリオ出力部 337 は、図 5 に示した第 1 の実施の形態のシナリオ検出部 130 内の同名の要素と同じ機能を有している。また、シナリオ検出部 330 には、イベント 81, 82, 83, . . . が順次入力され、不正アクセスを検出すると不正アクセスレポート 91, 92, 93, . . . が出力される。

【0110】

役割指定シナリオ定義 DB 331 は、予め定義された不正アクセスシナリオが定義されたデータベースである。ただし、役割指定シナリオ定義 DB 331 では、不正アクセスシナリオにおいて、関与する装置の役割が指定されている。たとえば、攻撃者のクライアントとしての役割、ハンドラとしての役割、エージェントとしての役割が指定されている。

【0111】

役割指定進行中シナリオ DB 332 は、役割が与えられた装置間で発生したイベントの遷移が進行中シナリオとして登録されたデータベースである。

役割指定進行中シナリオ検索部 334 は、関連ホスト抽出部 333 が抽出した「発信元 IP アドレス」「宛先 IP アドレス」をキーとして、何れかの IP アドレスの装置が関与している役割指定進行中シナリオ DB 332 を検索する。検出された役割指定進行中シナリオは、イベント系列照合部 335 に渡される。

【0112】

イベント系列照合部 335 は、役割指定進行中シナリオ検索部 334 により役割指定進行中シナリオ DB 332 から、該当するエントリが検出された場合、そのエントリが保持している「不正アクセスシナリオ名」、「進捗度」を取得する。そして、イベント系列照合部 335 は、役割指定シナリオ定義 DB 331 を参照し、入力されたイベントの名称により、入力されたイベントへの遷移が不正アクセスシナリオに沿っているかどうかを判定する。不正アクセスシナリオに沿ったイベントが発生していれば、その旨が役割指定進行中シナリオ更新部 336 に通知される。

【0113】

具体的には、イベント系列照合部 335 は、第 2 の実施の形態では各装置に役割が指定されているため、「発信元 IP アドレス」と「宛先 IP アドレス」とのそれぞれに対応する装置の役割を特定する。そして、イベント系列照合部 335 は、役割が特定された装置が、入力されたイベントにおいて、役割指定シナリオ定義 DB 331 で定義されている不正アクセスシナリオに沿った役割を担っている場合、シナリオが進行すると判断される。

【0114】

役割指定進行中シナリオ更新部 336 は、イベント系列照合部 335 においてシナリオが進行すると判断されたとき、役割指定進行中シナリオ DB 332 内の該当するエントリを更新する。具体的には、役割指定進行中シナリオ更新部 336 は、入力されたイベントから抽出された「発信元 IP アドレス」と「宛先 IP アドレス」とのそれぞれの役割を設定すると共に、シナリオの進捗度を 1 段階進める。

【0115】

図12は、役割指定シナリオ定義DBのデータ構造例を示す図である。役割指定シナリオ定義DB331には、不正アクセスシナリオ名とイベント遷移との項目が設けられている。不正アクセスシナリオ名には、DDoS攻撃のシナリオに設定された名称が登録される。イベント遷移には、イベント遷移によって表現されたDDoS攻撃のシナリオが登録される、イベント遷移の項目で登録されるイベントは、イベント名に加え、発信元と宛先との役割が設定される。このように、各イベントに「発信元」と「宛先」との装置に対し、「当該シナリオにおける役割」が関連付けられている。

【0116】

図12の例では、不正アクセスシナリオXのイベント遷移として、イベントa、イベントb、イベントcが登録されている。イベントaでは、発信元の役割はハンドラであり、宛先の役割はエージェントである。イベントbでは、発信元の役割はエージェントであり、宛先の役割はハンドラである。イベントcでは、発信元の役割はエージェントであり、宛先の役割はターゲットである。「ターゲット」とは不正アクセスの被害者である。

【0117】

このように、イベント毎に発信元と宛先とに対して役割が設定されている。ある装置（IPアドレスで識別される）に役割が一旦設定されると、その装置は、以後のイベントでも設定された通りの役割を担うことになる。たとえば、不正アクセスシナリオXのイベントaでは、発信元の装置がハンドラとなり、宛先の装置がエージェントとなる。そのため、次にイベントbが入力された場合、イベントaにおいてハンドラであった装置が宛先であり、イベントaにおいてエージェントであった装置が発信元である場合、そのシナリオが進行する。

【0118】

また、イベントcでは、新たな役割としてターゲットが出現する。したがって、イベントbでエージェントを担った装置が発信元となるイベントcが入力されれば、宛先に関係なくシナリオが進行する。

【0119】

図13は、役割指定進行中シナリオDBのデータ構造例を示す図である。役割指定進行中シナリオDB332には、役割担当IPアドレス、不正アクセスシナリオ名、および進捗度の項目が設けられている。

【0120】

役割担当IPアドレスの項目には、役割指定の進行中シナリオにおける最後のイベントでの各装置の役割が設定される。装置はIPアドレスによって特定される。なお、役割担当IPアドレスの項目に、過去に入力された全てのイベントにおける各装置の役割を設定しておいてもよい。

【0121】

不正アクセスシナリオ名の項目には、進行している不正アクセスシナリオの名称が登録される。

進捗度の項目には、進行中シナリオの進行の度合いが設定される。進捗度は、不正アクセスシーケンス上での何番目のイベントまで進行したのかによって示される。

【0122】

以上のような構成のシナリオ検出部330により、役割が指定された不正アクセスシナリオに沿って、3台以上の装置が役割に応じたイベントを発生させたとき、不正アクセスが検出される。具体的には、イベント81, 82, 83, ...が入力されると、入力されたイベント81, 82, 83, ...から、関連ホスト抽出部333によりキーデータが抽出される。キーデータは、発信元IPアドレスと宛先IPアドレスとである。

【0123】

すると、役割指定進行中シナリオ検索部334により、キーデータの少なくとも何れか一方の役割担当IPアドレスに設定されたエントリが、役割指定進行中シナリオDB332から検出される。検出されたエントリは、イベント系列照合部335に通知される。

【0124】

イベント系列照合部335では、役割指定シナリオ定義DB331が参照され、役割指定進行中シナリオ検索部334で検出されたエントリに対応する不正アクセスシナリオと、入力されたイベントとが照合される。入力されたイベントが、照合対象の不正アクセスシナリオに沿っていれば、シナリオが進行すると判断される。

【0125】

シナリオが進行すると判断された場合、役割指定進行中シナリオ更新部336により、役割指定進行中シナリオDB332内の該当エントリの進捗度が更新される。なお、入力されたイベントが、役割指定シナリオ定義DB331内の不正アクセスシナリオにおける先頭のイベントに相当するとき、役割指定進行中シナリオ更新部336は、新たなエントリを役割指定進行中シナリオDB332に追加する。

【0126】

また、イベント系列照合部335でシナリオを進行させると判断したとき、シナリオが最終端まで完了した場合、その旨が検出シナリオ出力部に通知される。すると、検出シナリオ出力部337が最終端まで完了したシナリオに関する不正アクセスレポートを出力する。

【0127】

このように、第2の実施の形態では、入力されたイベントと、その発信元の装置または宛先の装置が関連して現在進行している進行中シナリオとを、各ホストの役割までを鑑みて不正アクセスシナリオに符合するか否かを判定している。すなわち、不正アクセスシナリオにおいて、各イベントの送信元及び宛先の装置に「役割」を関連付けるものである。そのため、「2装置間による一方通行な不正アクセスシナリオ」に限らずDDoS攻撃のように、「双方向通信の含まれるシナリオ」「3者以上の装置が含まれる不正アクセスシナリオ」等を検出することが可能となる。

【0128】

[第3の実施の形態]

次に、第3の実施の形態について説明する。第3の実施の形態は、シナリオ定義DB中の、不正アクセスシナリオを示す「イベント遷移」を、「状態遷移」に拡張するためのものである。

【0129】

なお、第3の実施の形態における不正アクセス検知装置の機能の構成要素は、図4、図5に示す第1の実施の形態の構成要素とほぼ同じである。そこで、以下、図4、図5に示した構成を参照して、第1の実施の形態と異なる点について説明する。

【0130】

第3の実施の形態に係るシナリオ検出部130では、シナリオ定義DB131において、単純なイベントの遷移のみならず、イベントを契機とした状態遷移を格納する。そして、イベント系列照合部135において、現在の状態から、入力されたイベントによる遷移があるか否かを照合する。これにより、より複雑なシナリオを簡易に記述でき、攻撃モデルデータベースの縮小化が期待できる。

【0131】

図14は、第3の実施の形態のシナリオ定義DBに定義されるイベント遷移を示す図である。この例では、イベント遷移が、シナリオ状態遷移に置き換えて定義されている。シナリオの状態には、初期状態411、中間状態412、413、終了状態414がある。

【0132】

初期状態411から中間状態412へは、イベントaが入力されることで遷移する。初期状態411から中間状態413へは、イベントbが入力されることで遷移する。

中間状態412から中間状態413へは、イベントcが発生することで遷移する。中間状態412から終了状態414へは、イベントdが発生することで遷移する。中間状態413から終了状態414へは、イベントfが発生することで遷移する。中間状態413のときにイベントeが発生すると、中間状態413が維持される。

【0133】

このように、第3の実施の形態では、状態遷移の遷移条件がイベントとなっている。これにより、イベントとシナリオを照合することができる。

なお、状態遷移においては、イベント遷移の先頭に該当する「初期状態」と、終端に該当する「終了状態」が含まれる必要がある。

【0134】

また、第3の実施の形態における不正アクセス検知装置の進行中シナリオDB132では、各エントリにおいて「進捗度」を「状態名」（図14の例では中間状態412など）で表すこととなる。

【0135】

〔第4の実施の形態〕

次に、第4の実施の形態について説明する。第4の実施の形態では、シナリオ定義データベースに格納されたイベント遷移あるいはイベントを契機とした状態遷移において、遷移それぞれに予め有効期限を設定しておく。そして、現在処理中のイベントと、そのキーデータが関連した進行中シナリオを、各遷移の有効期限までを鑑みてイベント遷移若しくは状態遷移に符合するか否かを判定する。すなわち、入力されたイベントと進行中シナリオとのキーデータが一致しても、進行中シナリオの有効期限を超えていれば、イベントは進行しない。これにより、有効期限以上に発生間隔の離れたイベント同士は、別のシナリオとして処理することができる。

【0136】

なお、第4の実施の形態における不正アクセス検知装置の機能の構成要素は、図4、図5に示す第1の実施の形態の構成要素とはほぼ同じである。そこで、以下、図4、図5に示した構成を参照して、第1の実施の形態と異なる点について説明する。

【0137】

図15は、第4の実施の形態のシナリオ定義DBに定義されるイベント遷移を示す図である。図15に示すように、イベント421～423の配列でイベント遷移が定義されている。また、シナリオが進行する際の有効期限424、425が設定されている。

【0138】

具体的には、イベント421からイベント422へ遷移する際の有効期限424は、5分である。また、イベント422からイベント423へ遷移する際の有効期限425は、1時間である。

【0139】

このように、攻撃モデルを示す不正アクセスシナリオ中のイベント間の遷移に「有効期限」が関連付けられ、進行中シナリオDB132中の各エントリにおいて、「前の遷移が発生した時刻」を保持する。イベント系列照合部135は、不正アクセスシナリオ中の「有効期限」、進行中シナリオ中の「前の遷移が発生した時刻」及び現在時刻を照合して、遷移が発生するか否かを判定する。

【0140】

たとえば、「前の遷移が発生した時刻」が正午であり、その次の遷移の有効期限が5分だった場合、次のイベントの入力が12時5分以内であればそれに係る遷移は有効となり、12時5分を過ぎていればそれに係る遷移は無効となる。

【0141】

このように、シナリオの進行に有効期限を設けることで、誤った不正アクセスを検出することを防止することができる。

また、進行中シナリオ更新部136は、進行中シナリオDB132から、有効期限の切れた不要なエントリを削除することができる。この場合、進行中シナリオDB132は、シナリオ定義DB131中の「有効期限」、進行中シナリオDB132中の「前の遷移が発生した時刻」、及び現在時刻を鑑みて、適当なタイミング（たとえば、所定の時間間隔）で有効期限が切れたエントリを進行中シナリオDB132から消去する。

【0142】

たとえば、進行中シナリオDB132は、10分ごとに進行中シナリオDB132中の有効期限の切れたシナリオを全検索する。そして、進行中シナリオDB132は、検出された進行中シナリオのエントリを進行中シナリオDB132より削除する。これにより、有効期限の切れたシナリオを10分以内に削除できる。

【0143】

このように、有効期限切れの進行中シナリオを削除することで、途中まで進んだ攻撃が止まった進行中シナリオによって進行中シナリオDB132が溢れてしまう事態を回避できる。

【0144】

〔第5の実施の形態〕

次に、第5の実施の形態について説明する。第5の実施の形態では、不正アクセスシナリオの途中の段階まで進行中シナリオが進行したとき、不正アクセスの発生の予兆を通知する不正アクセスレポートを出力する。不正アクセスの予兆は、進行中シナリオが進行する毎に加算される重みによって判断する。すなわち、進行中シナリオの重みのトータルが所定値を超えたときに、不正アクセスの予兆有りと判断される。

【0145】

すなわち、第1～第4の実施の形態では、進行中シナリオが不正アクセスシナリオの終端に達したとき、不正アクセス検出のレポートを出力していた。ところが、不正アクセスシナリオの途中まで進行中シナリオが進行すれば、最終的に攻撃が実行される蓋然性が高いと判断できることがある。そこで、第5の実施の形態では、将来的に攻撃が行われる蓋然性が高いと判断できるときは、これはシナリオの途中の段階でもレポートを出力する。

【0146】

なお、第5の実施の形態における不正アクセス検知装置の機能の構成要素は、図4、図5に示す第1の実施の形態の構成要素とほぼ同じである。そこで、以下、図4、図5に示した構成を参照して、第1の実施の形態と異なる点について説明する。

【0147】

第5の実施の形態では、シナリオ定義DB131において、予めイベント遷移や状態遷移の各イベントや遷移に重みを付与しておく。

図16は、第5の実施の形態のイベント遷移DBに設定されるイベント遷移の例を示す図である。図16に示すようにイベント遷移を構成する各イベント431～433には、重み434～436が設定されている。たとえば、イベント431の重みは1であり、イベント432の重みは5であり、イベント433の重みは3である。

【0148】

また、イベント432は、繰り返し発生することがある。たとえば、ポートスキャンのイベントなどは、繰り返し発生する。

そして、不正アクセスシナリオのイベント遷移には、レポート出力閾値が設定されている。レポート出力閾値は、攻撃が行われる蓋然性の有無を判断するための指標である。発生したイベントの重みのトータルがレポート出力閾値を超えたとき、攻撃が行われる予兆有りと判断され、レポート提出が行われる。

【0149】

イベントに重みが設定されることにより、進行中シナリオDB132には、進捗度の項目に代えて、重みトータルの項目が設けられる。

図17は、第5の実施の形態における進行中シナリオDBのデータ構造例を示す図である。第5の実施の形態における進行中シナリオDB132aには、発信元IPアドレスと宛先IPアドレスとの組、不正アクセスシナリオ名、および重みトータルの項目が設けられている。重みトータルには、対応する進行中シナリオにおいて発生したイベントに設定されている重みのトータルが設定される。

【0150】

イベント系列照合部135は、イベントが入力されることで進行中シナリオが進行したとき、入力されたイベントの重みを、対象となる進行中シナリオの重みトータルに加算す

る。そして、加算した後の重みトータルが不正アクセスシナリオのレポート出力閾値を超えたとき、イベント系列照合部 135 は、不正アクセスの発生確率が高いと判断し、その旨を検出シナリオ出力部 137 に伝える。すると、検出シナリオ出力部 137 は、不正アクセスを検出したとして不正アクセスレポートを出力する。

【0151】

たとえば、図 16 に示すイベント遷移の場合、イベント 431 からイベント 432 に遷移した段階では、重みトータルは「6」であり、レポートは出力されない。その後、イベント 433 が再度発生した場合、重みトータルが「9」となり、レポート出力閾値「8」を超える。したがって、不正アクセスレポートが出力される。

【0152】

また、イベント 431 からイベント 432 に遷移し、その後、再度イベント 432 が入力された場合、重みトータルが「11」となる。この場合にも重みトータルがレポート出力閾値「8」を超えることとなり、不正アクセスレポートが出力される。

【0153】

なお、進行中シナリオが進行したときは、進行中シナリオ更新部 136 によって、進行中シナリオ DB 132 内の該当エントリにおける重みトータルの値が更新される。すなわち、新たに発生したイベントの重みが、元の重みトータルの値に加算される。

【0154】

このように、重みによって不正アクセスの蓋然性を判断できるようにすることで、実際に攻撃が行われる前に、不正アクセスレポートを出力し、システムの管理者に警告を発することができる。

【0155】

なお、重みを用いずに、進捗度によって、攻撃の予兆を通知する不正アクセスレポートを出力することもできる。たとえば、不正アクセスシナリオ毎に、何番目のイベントを超えたらレポート出力を行うのかを、閾値として設定しておく。イベント系列照合部 135 は、進行中シナリオの進捗度が閾値を超えたとき、その旨を検出シナリオ出力部 137 に通知する。すると、検出シナリオ出力部 137 において不正アクセスレポートが出力される。

【0156】

〔第 6 の実施の形態〕

第 6 の実施の形態は、不正アクセスシナリオにおいて、その状態、含まれるイベント、及びそれに付随するパラメータなどを鑑み、将来起こりうる被害の種類、大きさ等を予測するものである。しかも、予測内容に応じて事前の予防対策を自動的に実施することもできる。

【0157】

すなわち、イベント系列で定義された不正アクセスシナリオに沿った進行中シナリオの進行過程で、不正アクセスシナリオ上の以後のイベント遷移を参照することで、将来起こりうるイベントを予測することもできる。しかし、将来起こるイベントが分かっても、それが効果的な不正アクセス回避に繋がるとは限らない。むしろ、将来起こりうる被害の種類、大きさ、時間、期間などが分かったほうが、効果的な不正アクセス回避を行うことができる。

【0158】

図 18 は、第 6 の実施の形態に係る不正アクセス検知装置の内部構成を示すブロック図である。不正アクセス検知装置 500 は、通信処理部 510、パケットモニタ部 520、シナリオ検出部 530、引数抽出部 540、攻撃レポート部 550 および事前対策実施部 560 を有している。

【0159】

通信処理部 510 は、パケットモニタ部 520、引数抽出部 540、および攻撃レポート部 550 については、図 10 に示した第 2 の実施の形態の同名の構成要素と同様の機能を有している。シナリオ検出部 530 は、パケットモニタ部 520 で検出されたイベント

に基づいて、不正アクセスシナリオに沿ったイベント遷移を検出する。そして、不正アクセスシナリオに沿ったイベント遷移に基づいて、不正アクセスの予備動作の進行状況に応じて、攻撃の可能性や被害の大きさを予測する。そして、シナリオ検出部 530 は、予測結果を攻撃レポート部 550 に通知する。また、シナリオ検出部 530 は、予測により事前対策が必要と判断された場合、対策要求を事前対策実施部 560 に通知する。

【0160】

事前対策実施部 560 は、シナリオ検出部からの対策要求に応じて、攻撃を抑止するための事前対策を実行する。たとえば、不正アクセスの予兆を検出したら、当該通信を以後所定の時間遮断する。

【0161】

このような構成の不正アクセス検知装置 500 により、不正アクセスの予兆を検知し、攻撃レポート 571, 572, 573, ... を出力する共に、事前対策を施すことができる。

【0162】

図 19 は、第 6 の実施の形態のシナリオ検出部の機能を示すブロック図である。シナリオ検出部 530 は、役割指定シナリオ定義データベース (DB) 531、役割指定進行中シナリオ DB 532、関連ホスト抽出部 533、役割指定進行中シナリオ検索部 534、イベント系列照合部 535、役割指定進行中シナリオ更新部 536、検出シナリオ出力部 537 および対策指示部 538 を有している。

【0163】

役割指定シナリオ定義 DB 531、役割指定進行中シナリオ DB 532、関連ホスト抽出部 533、役割指定進行中シナリオ検索部 534、イベント系列照合部 535、役割指定進行中シナリオ更新部 536、および検出シナリオ出力部 537 は、図 11 に示した第 2 の実施の形態の同名の構成要素とほぼ同じ機能を有している。以下、これらの構成要素のうち第 2 の実施の形態と異なる機能について説明するとともに、対策指示部 538 の機能を説明する。

【0164】

イベント系列照合部 535 は、役割が指定された不正アクセスシナリオと、進行中シナリオから入力されたイベントに応じた状態遷移との照合を行う。その際、イベント系列照合部 535 は、予め状態毎に設定されている予測インパクト／対策定義テーブルを参照して、インパクト（攻撃開始）までの予想時間、その時間内のインパクトの発生確率、およびインパクトの大きさを判断する。そして、イベント系列照合部 535 は、予想される攻撃の内容に応じた対策を決定する。緊急を要する対策であれば、対策指示部 538 に対して対策の内容が通知される。緊急を要さない対策であれば、検出シナリオ出力部 537 に対策の内容が通知される。

【0165】

検出シナリオ出力部 537 は、予想される攻撃の内容を受け取った場合、その攻撃に関する不正アクセスレポートを出力する。出力された不正アクセスレポートは、攻撃レポート部 550 によって、不正アクセス検知装置 500、攻撃の対象となる装置、攻撃の踏み台となる装置等のそれぞれの管理者に通知される。

【0166】

対策指示部 538 は、イベント系列照合部 535 から対策内容を受け取ると、その内容の対策要求 620 を生成し、事前対策実施部 560 に渡す。すると、事前対策実施部 560 によって、所定の通信の遮断等の対策が実施される。

【0167】

また、第 6 の実施の形態では、役割指定シナリオ定義 DB 531 は、図 14 と同様な状態遷移によって不正アクセスシナリオが定義されている。たとえば、著名な DDOS 発生ツールである Trinoo に応じた不正アクセスシナリオを役割指定シナリオ定義 DB 531 に登録することができる。

【0168】

図20は、Trinooに対する設定コマンドを示す図である。図20に示すハンドラ向けコマンドは、攻撃者が、ハンドラに対して入力するコマンドである。エージェント向けコマンドは、入力されたコマンドに応答してハンドラがエージェントに対して送信するコマンドである。攻撃者が、ハンドラに対して図20の上に記載されているコマンドから順に入力することで、パケットフラッドによる攻撃を指示することができる。

【0169】

たとえば、攻撃者が「msize」を入力すると、ハンドラからエージェントに「rsz」が送信される。このコマンドは、エージェントに対して、将来発生させるパケットフラッド中の、UDPパケットのサイズ(Byte)を引数で設定することを指示している。

【0170】

攻撃者が「mtimer」を入力すると、ハンドラからエージェントに「bbb」が送信される。このコマンドは、エージェントに対して、将来発生させるフラッドの長さ(秒)を引数で設定することを指示している。

【0171】

攻撃者が「mping」を入力すると、ハンドラからエージェントに「png」が送信される。このコマンドは、全てのエージェントの生死(起動されているか否か)を確認するためのコマンドである。起動されているエージェントのみが、「png」に対して応答を返す。

【0172】

攻撃者が「die」を入力すると、ハンドラからエージェントに「dle」が送信される。このコマンドは、全てのエージェントに対して動作の停止を指示している。

攻撃者が「dos」を入力すると、ハンドラからエージェントに「aaa」が送信される。このコマンドは、エージェントに対して、引数指定したIPアドレスにUDPフラッドを発信ことを指示している。

【0173】

攻撃者が「mdos」を入力すると、ハンドラからエージェントに「xyz」が送信される。このコマンドは、エージェントに対して、引数指定したIPアドレスにUDPフラッドを発信することを指示している。この場合、UDPフラッドを発信する対象として、複数のIPアドレスを指定することもできる。

【0174】

これらの指示がハンドラからエージェントに伝えられることで、エージェントによるウェブサーバ等への攻撃が実行される。

そこで、役割指定シナリオ定義DB531には、図20に示すコマンドに応じたイベント遷移が不正アクセスシナリオとして登録される。

【0175】

図21は、Trinooに応じた不正アクセスシナリオのイベント遷移を示す図である。この例では、イベント遷移が初期状態631、中間状態632～634、および終了状態635、636で示されている。

【0176】

図21では、エージェント起動メッセージのイベントが実線の矢印で示されている。設定コマンドのイベントは、点線の矢印で示されている。PONG(pingへの応答)のイベントは、破線の矢印で示されている。攻撃命令のイベントは、1点鎖線の矢印で示されている。終了命令のイベントは、2点鎖線の矢印で示されている。

【0177】

初期状態631(「agent_start(エージェント起動)」の指示待機状態)からエージェント起動メッセージが出力されると、中間状態632に状態が遷移する。

中間状態632は、「config_waiting(攻撃態勢完了待ち)」の状態である。中間状態632は、攻撃の準備が整っていないため、フラッドが直ぐに発生する可能性は低いと考えられる。中間状態632から設定コマンドが発行されると、中間状態633に状態が遷移する。また、中間状態632からPONGが発行されると、中間状態634に状態が遷移する。さらに、中間状態632から攻撃命令が発行されると、終了状態636に状態

が遷移する。

【0178】

中間状態633は、「configured (攻撃態勢完了)」の状態である。中間状態633では、パケットフラッドによる攻撃が直ぐに発生する可能性がやや高いと考えられる。中間状態633から攻撃指令が発効されると、終了状態636に状態が遷移する。また、中間状態633から終了命令が発効されると、終了状態635に状態が遷移する。さらに、中間状態633からPONGが発行されると、中間状態634に状態が遷移する。

【0179】

中間状態634は、「UDP_waiting (UDPフラッド開始指示待ち)」の状態である。中間状態634では、パケットフラッドによる攻撃が直ぐに発生する可能性が高いと考えられる。中間状態634から攻撃指令が発効されると、終了状態636に状態が遷移する。また、中間状態633から終了命令が発効されると、終了状態635に状態が遷移する。さらに、中間状態634から設定コマンドが発行されると、中間状態633に状態が遷移する。

【0180】

終了状態635は、「died (エージェント停止)」の状態である。終了状態635になれば、少なくともこの進行中シナリオによってパケットフラッドが発生する可能性がなくなる。

【0181】

終了状態636は、「UDP_flooding (フラッド実行)」の状態である。終了状態636の時点では、パケットフラディングによる攻撃が既に開始されている。

このように、Trinooと呼ばれるツールはコマンドベースで動作し、各コマンドに与える引数を監視することによって、最終的な被害に関する情報(DDoS攻撃の時間、パケットサイズ、等)を類推できる。なお、DDoS攻撃は、いったん攻撃が開始されると被害を回避することは困難と言われている。したがって、DDoS攻撃を予測することで、DDoS攻撃が発生する前に段階的且つ柔軟な対策を選択・実施することが必要である。

【0182】

第6の実施の形態では、各状態に対応付けて、その状態のときの予測インパクト/対策定義テーブルが予め設定されている。

図22は、「UDP_waiting」の状態に対応する予測インパクト/対策定義テーブルの例を示す図である。予測インパクト/対策定義テーブル640には、予測インパクトとして、インパクト(攻撃)までの時間、インパクトの発生確率、インパクトの大きさが設定されている。なお、インパクトの大きさは、「大」、「中」、「小」の3段階で示されている。また、予測インパクトに対して、実施する対策が設定されている。

【0183】

図22の例では、5分以内にインパクトがある確率は70%であり、そのときのインパクトの大きさは「大」である。1時間以内にインパクトがある確率は10%であり、そのときのインパクトの大きさは「大」である。1日以内にインパクトがある確率は10%であり、そのときのインパクトの大きさは「中」である。

【0184】

このような予測インパクトの場合、緊急性が高くインパクトも大きいため、当該通信を以後一時間遮断するという実施対策となる。この実施対策を自動実行する場合、通信の遮断を指示する対策要求620が事前対策実施部560に通知される。すると、事前対策実施部560によって、たとえば、ハンドラとエージェントとの間の通信が遮断される。

【0185】

図23は、「config_waiting」の状態に対応する予測インパクト/対策定義テーブルの例を示す図である。この予測インパクト/対策定義テーブル650によれば、1時間以内にインパクトがある確率は10%であり、そのときのインパクトの大きさは「中」である。1日以内にインパクトがある確率は40%であり、そのときのインパクトの大きさは「大」である。3日以内にインパクトがある確率は30%であり、そのときのインパクト

の大きさは「大」である。

【0186】

このような予測インパクトの場合、図22に比べ、比較的対策時間に余裕がある（緊急性は低い）。そこで、対策として、攻撃を起こしそうなホストの管理者（管理ホスト）に連絡する。また、当該通信を、以後3日間監視し、必要に応じて遮断する。この実施対策を自動実行する場合、通信の遮断を指示する対策要求620が事前対策実施部560に通知される。すると、事前対策実施部560によって、たとえば、通信の監視が行われる。

【0187】

なお、DDoS攻撃のエージェントの種類及びその位置（装置のIPアドレス等）を特定できた場合、当該装置や周囲のネットワークのスペックを取得し併せて分析することで、DDoS攻撃の浪費帯域等について予測を行うこともできる。

【産業上の利用可能性】

【0188】

なお、上記の実施の形態では、不正アクセス検知装置を単体の装置として説明したが、不正アクセス検知装置の機能をファイアウォールやその他のコンピュータに内蔵することもできる。

【0189】

上記の処理機能は、コンピュータによって実現することができる。その場合、不正アクセス検知装置が有すべき機能の処理内容を記述したプログラムが提供される。そのプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリなどがある。磁気記録装置には、ハードディスク装置（HDD）、フレキシブルディスク（FD）、磁気テープなどがある。光ディスクには、DVD（Digital Versatile Disc）、DVD-RAM（Random Access Memory）、CD-ROM（Compact Disc Read Only Memory）、CD-R（Recordable）／RW（ReWritable）などがある。光磁気記録媒体には、MO（Magneto-Optical disk）などがある。

【0190】

プログラムを流通させる場合には、たとえば、そのプログラムが記録されたDVD、CD-ROMなどの可搬型記録媒体が販売される。また、プログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することもできる。

【0191】

プログラムを実行するコンピュータは、たとえば、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、自己の記憶装置に格納する。そして、コンピュータは、自己の記憶装置からプログラムを読み取り、プログラムに従った処理を実行する。なお、コンピュータは、可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することもできる。また、コンピュータは、サーバコンピュータからプログラムが転送される毎に、逐次、受け取ったプログラムに従った処理を実行することもできる。

【0192】

（付記1） ネットワークを介した不正アクセスを検出するための不正アクセス検知装置において、

準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段と

、
前記不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する進行中シナリオ記憶手段と、

前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから前記キーデータを抽出するキーデータ抽出手段と、

前記キーデータ抽出手段が抽出した前記キーデータを検索キーとして、前記進行中シナリオ記憶手段から前記進行中シナリオを検索する進行中シナリオ検索手段と、

前記進行中シナリオ検索手段で検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが、前記不正アクセスシナリオ記憶手段に格納されている前記不正アクセスシナリオに沿っているかどうかを照合する照合手段と、

前記照合手段による照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シナリオを更新する進行中シナリオ更新手段と、

前記照合手段による照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力するレポート出力手段と、

を有することを特徴とする不正アクセス検知装置。

【0193】

(付記2) 前記レポート出力手段は、前記進行中シナリオ検索手段で検出された前記進行中シナリオが、前記不正アクセスシナリオの最後の処理まで進行したときに前記不正アクセスレポートを出力することを特徴とする付記1記載の不正アクセス検知装置。

【0194】

(付記3) 前記進行中シナリオ記憶手段は、前記進行中シナリオに対応付けて、前記進行中シナリオの進捗度を示す数値を記憶しており、

前記進行中シナリオ更新手段は、前記進捗度の数値を増加させることで、前記進行中シナリオを更新することを特徴とする付記1記載の不正アクセス検知装置。

【0195】

(付記4) 前記レポート出力手段は、前記進捗度が所定の値を超えたとき、前記不正アクセスレポートを出力することを特徴とする付記4記載の不正アクセス検知装置。

(付記5) 前記不正アクセスシナリオ記憶手段では、前記不正アクセスシナリオに関し、前記ネットワークを介して行われる処理を示す情報の発信元と宛先とのそれぞれに対して役割が設定されており、

前記照合手段は、前記パケットで示される処理の発信元と宛先とが、前記不正アクセスシナリオで定義された役割を担っているかどうかを判定することを特徴とする付記1記載の不正アクセス検知装置。

【0196】

(付記6) 前記不正アクセスシナリオ記憶手段に格納された前記不正アクセスシナリオは、前記ネットワークを介して行われる処理の指示や応答の際に発生するイベントを契機とした状態遷移によって、準備動作を経て不正アクセスが実行されるまでの処理手順が定義されており、

前記照合手段は、前記パケットで示される処理のイベントによる状態遷移が、前記不正アクセスシナリオに沿っているか否かを判定することを特徴とする付記1記載の不正アクセス検知装置。

【0197】

(付記7) 前記不正アクセスシナリオ記憶手段に格納された前記不正アクセスシナリオは、処理が次の段階へ進行するまでの有効期限が設定されており、

前記照合手段は、前記パケットで示される処理が、前記有効期限内に発生した処理かどうかを判定することを特徴とする付記1記載の不正アクセス検知装置。

【0198】

(付記8) 前記不正アクセスシナリオ記憶手段に格納された前記不正アクセスシナリオは、シナリオが進行する毎に加算される重みが定義されており、

前記レポート出力手段は、重みのトータルが所定値を超えたとき、前記不正アクセスレポートを出力することを特徴とする付記1記載の不正アクセス検知装置。

【0199】

(付記 9) ネットワークを介した不正アクセスを検出するための不正アクセス検知方法において、

前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから所定のキーデータを抽出し、

準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するための前記キーデータに対応付けて格納する進行中シナリオ記憶手段から、前記パケットから抽出した前記キーデータを検索キーとして前記進行中シナリオを検索し、

前記不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段を参照し、検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが前記不正アクセスシナリオに沿っているかどうかを照合し、

照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シナリオを更新し、

照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力する、

ことを特徴とする不正アクセス検知方法。

【0200】

(付記 10) ネットワークを介した不正アクセスを検出するための不正アクセス検知プログラムにおいて、

コンピュータを、

準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段、

前記不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する進行中シナリオ記憶手段、

前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから前記キーデータを抽出するキーデータ抽出手段、

前記キーデータ抽出手段が抽出した前記キーデータを検索キーとして、前記進行中シナリオ記憶手段から前記進行中シナリオを検索する進行中シナリオ検索手段、

前記進行中シナリオ検索手段で検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが、前記不正アクセスシナリオ記憶手段に格納されている前記不正アクセスシナリオに沿っているかどうかを照合する照合手段、

前記照合手段による照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シナリオを更新する進行中シナリオ更新手段、

前記照合手段による照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力するレポート出力手段、

として機能させるための不正アクセス検知プログラム。

【0201】

(付記 11) ネットワークを介した不正アクセスを検出するための不正アクセス検知プログラムを記録したコンピュータ読み取り可能な記録媒体において、

コンピュータを、

準備動作を経て不正アクセスが実行されるまでに前記ネットワークを介して行われる処理の手順を定義した不正アクセスシナリオが格納された不正アクセスシナリオ記憶手段、

前記不正アクセスシナリオに沿って前記ネットワークを介して行われた処理の経過を示す進行中シナリオを、前記進行中シナリオに関連する処理と他の処理とを区別するためのキーデータに対応付けて格納する進行中シナリオ記憶手段、

前記ネットワークを介して通信されるパケットを取得し、取得した前記パケットから前記キーデータを抽出するキーデータ抽出手段、

前記キーデータ抽出手段が抽出した前記キーデータを検索キーとして、前記進行中シナリオ記憶手段から前記進行中シナリオを検索する進行中シナリオ検索手段、

前記進行中シナリオ検索手段で検出された前記進行中シナリオに続けて前記パケットで示される処理を行うことが、前記不正アクセスシナリオ記憶手段に格納されている前記不正アクセスシナリオに沿っているかどうかを照合する照合手段、

前記照合手段による照合の結果、前記不正アクセスシナリオに沿っていると判断されたとき、前記進行中シナリオ記憶手段に格納されている前記進行中シナリオを更新する進行中シナリオ更新手段、

前記照合手段による照合の結果に基づいて、前記不正アクセスシナリオに沿った処理の進行状況を示す不正アクセスレポートを出力するレポート出力手段、

として機能させるための不正アクセス検知プログラムを記録したコンピュータ読み取り可能な記録媒体。

【図面の簡単な説明】

【0202】

【図1】実施の形態に適用される発明の概念図である。

【図2】第1の実施の形態に係るネットワークシステムの構成例を示す図である。

【図3】本発明の実施の形態に用いる不正アクセス検知装置のハードウェア構成例を示す図である。

【図4】第1の実施の形態に係る不正アクセス検知装置の内部構成を示すブロック図である。

【図5】第1の実施の形態のシナリオ検出部の機能を示すブロック図である。

【図6】シナリオ定義DBのデータ構造例を示す図である。

【図7】進行中シナリオDBのデータ構造例を示す図である。

【図8】シナリオ検出処理の手順を示すフローチャートである。

【図9】DDoS攻撃の発生メカニズムを示す概念図である。

【図10】第2の実施の形態に係る不正アクセス検知装置の内部構成を示すブロック図である。

【図11】第2の実施の形態のシナリオ検出部の機能を示すブロック図である。

【図12】役割指定シナリオ定義DBのデータ構造例を示す図である。

【図13】役割指定進行中シナリオDBのデータ構造例を示す図である。

【図14】第3の実施の形態のシナリオ定義DBに定義されるイベント遷移を示す図である。

【図15】第4の実施の形態のシナリオ定義DBに定義されるイベント遷移を示す図である。

【図16】第5の実施の形態のイベント遷移DBに設定されるイベント遷移の例を示す図である。

【図17】第5の実施の形態における進行中シナリオDBのデータ構造例を示す図である。

【図18】第6の実施の形態に係る不正アクセス検知装置の内部構成を示すブロック図である。

【図19】第6の実施の形態のシナリオ検出部の機能を示すブロック図である。

【図20】Trinooに対する設定コマンドを示す図である。

【図21】Trinooに応じた不正アクセスシナリオのイベント遷移を示す図である。

【図22】「UDP_waiting」の状態に対応する予測インパクト/対策定義テーブルの例を示す図である。

【図23】「config_waiting」の状態に対応する予測インパクト/対策定義テーブルの例を示す図である。

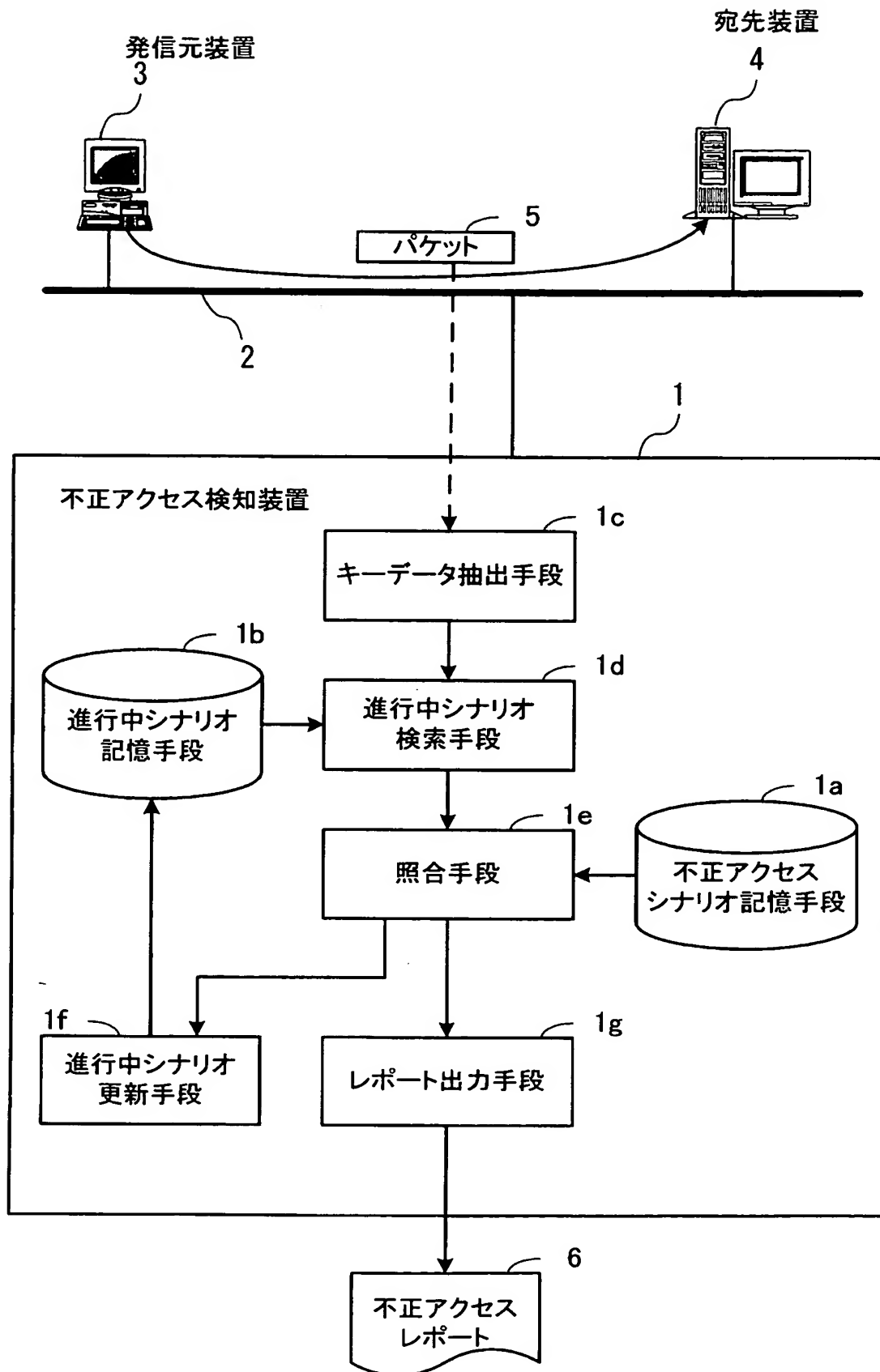
【符号の説明】

【0203】

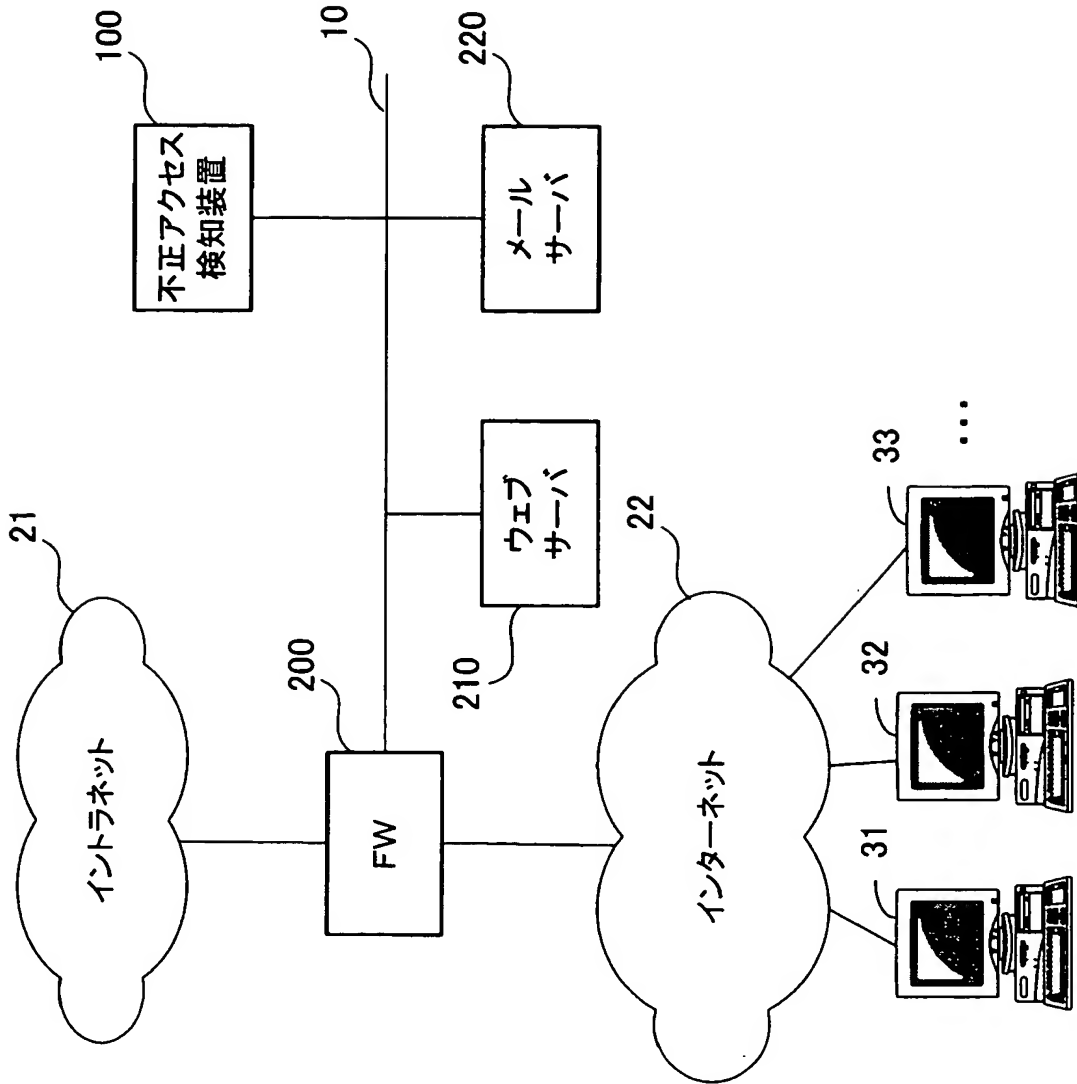
1 不正アクセス検知装置

- 1 a 不正アクセスシナリオ記憶手段
- 1 b 進行中シナリオ記憶手段
- 1 c キーデータ抽出手段
- 1 d 進行中シナリオ検索手段
- 1 e 照合手段
- 1 f 進行中シナリオ更新手段
- 1 g レポート出力手段
- 2 ネットワーク
- 3 発信元装置
- 4 宛先装置
- 5 パケット
- 6 不正アクセスレポート

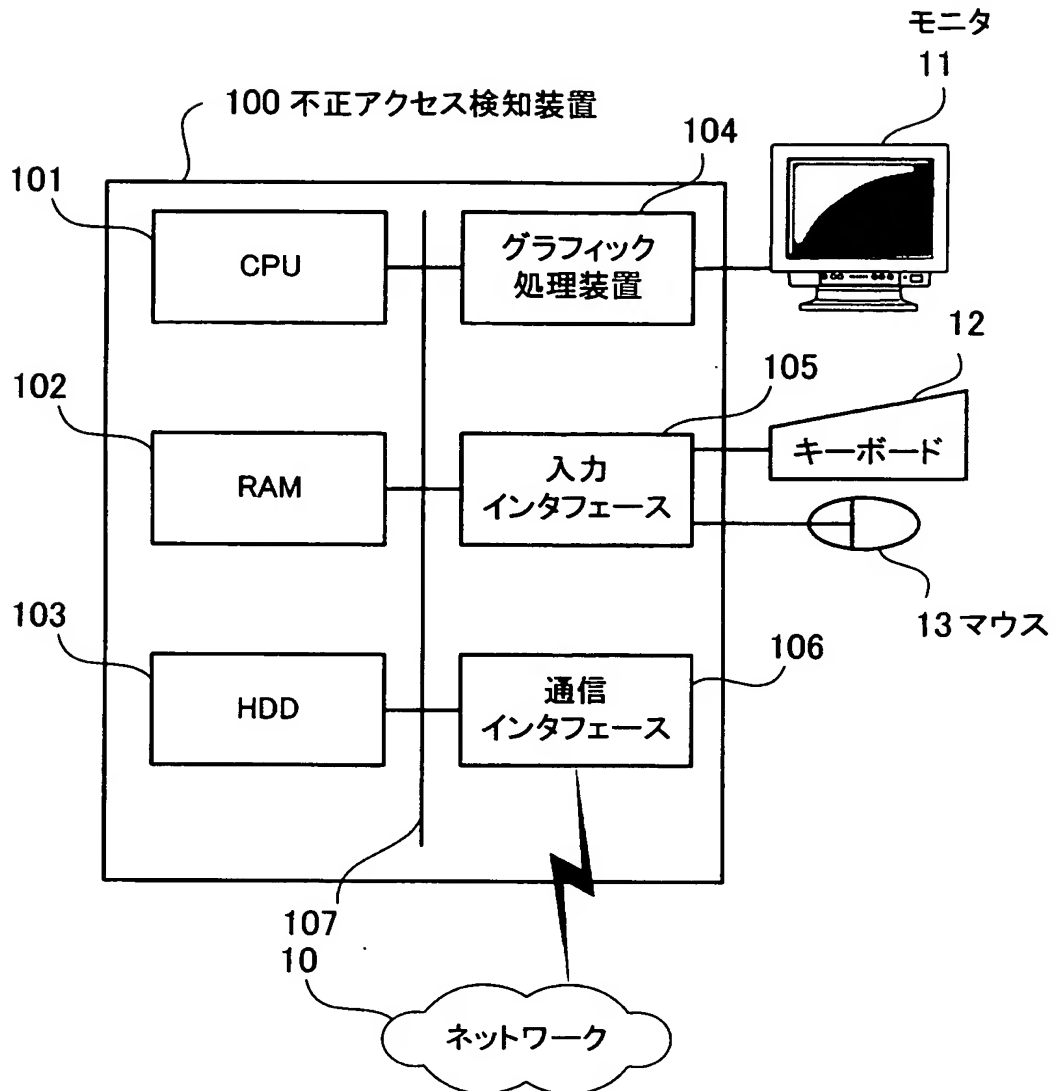
【書類名】 図面
【図 1】



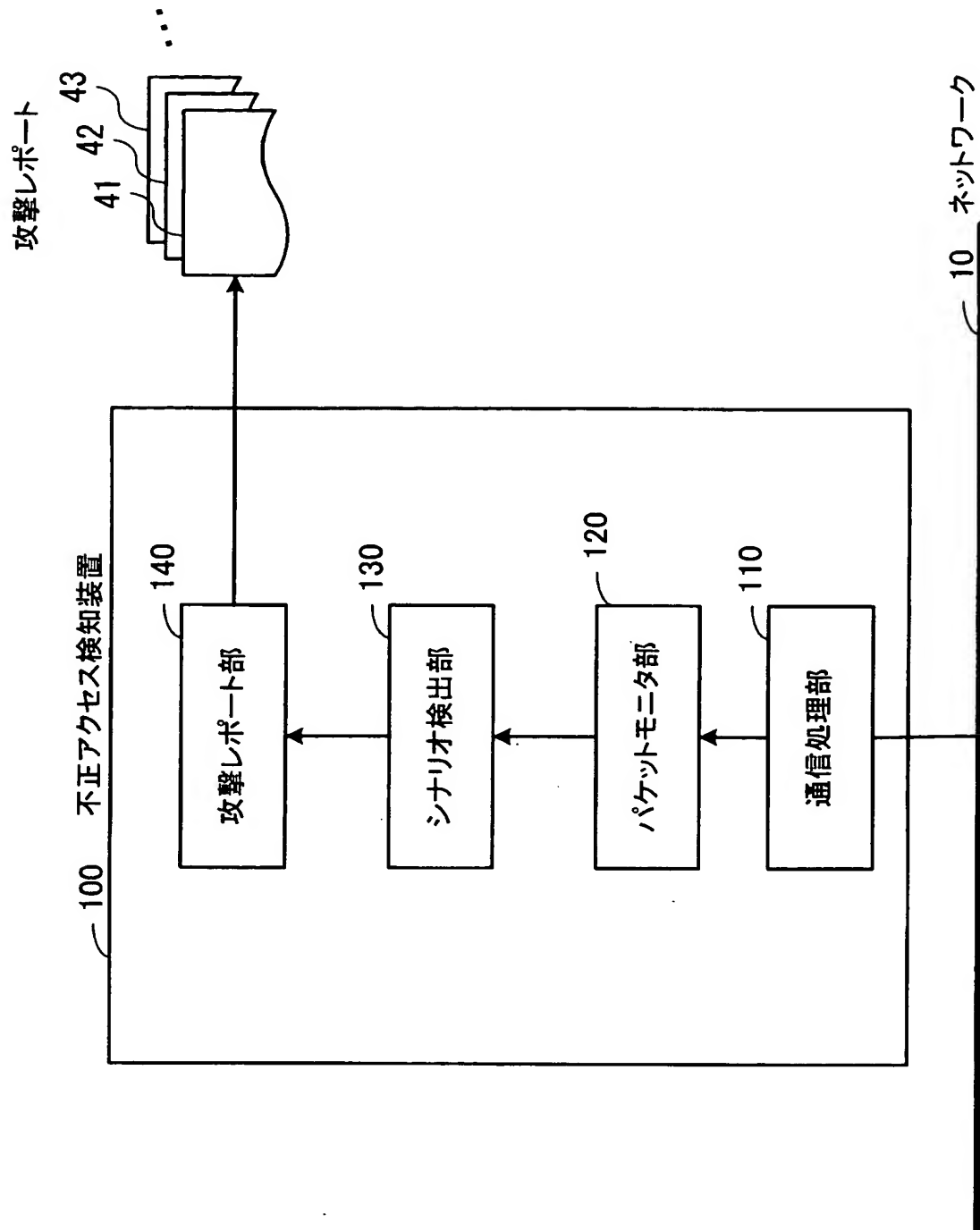
【図 2】



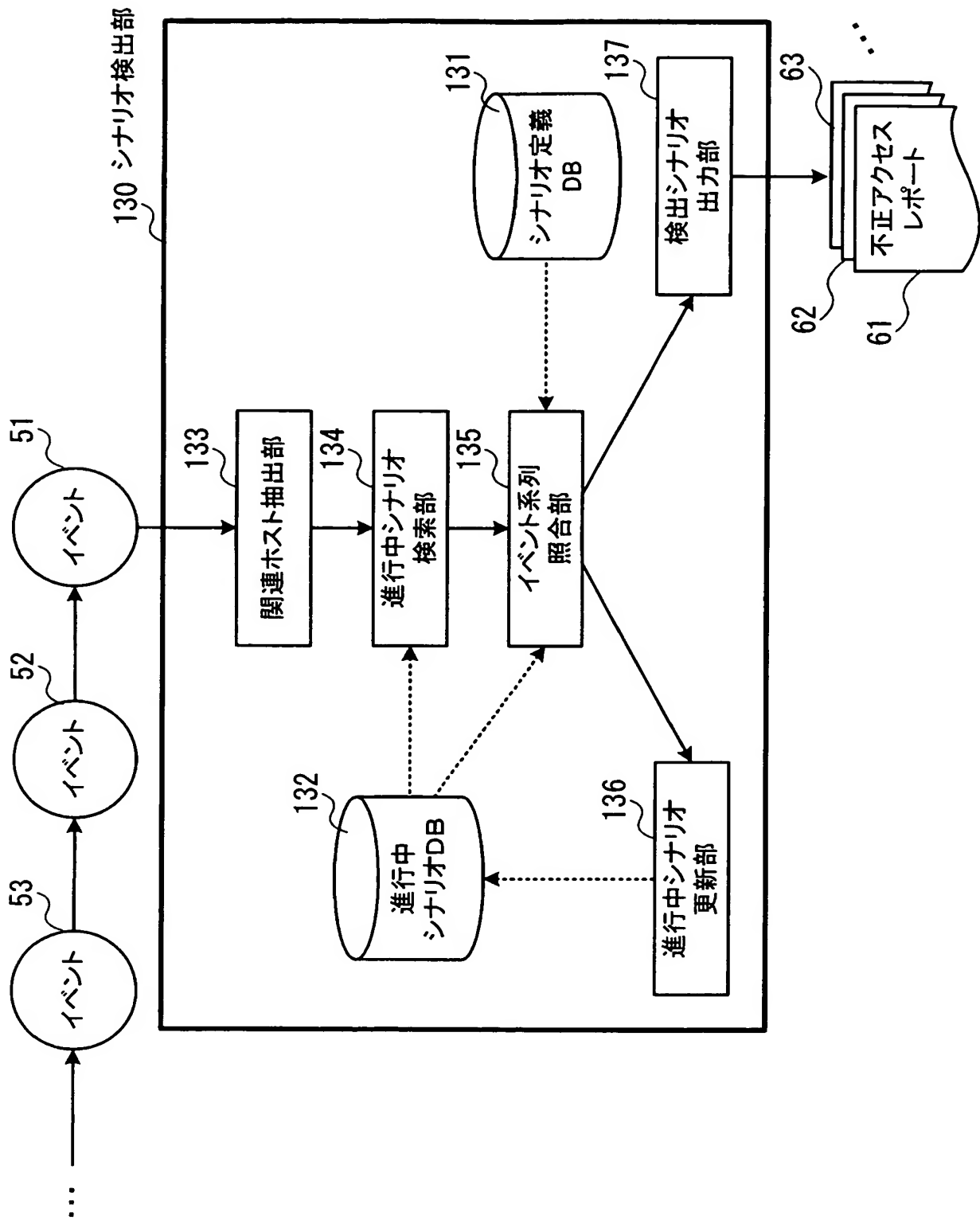
【図 3】



【図 4】

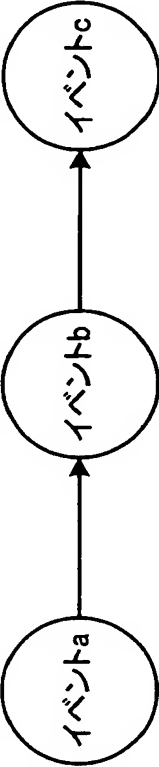
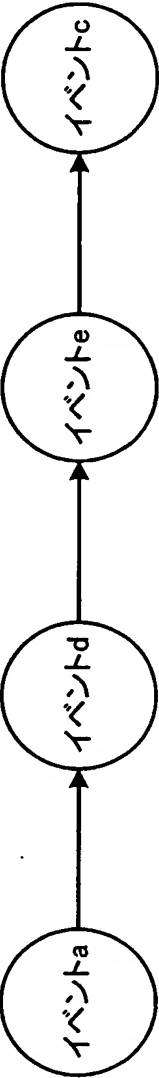


【図 5】



【図 6】

131 シナリオ定義DB

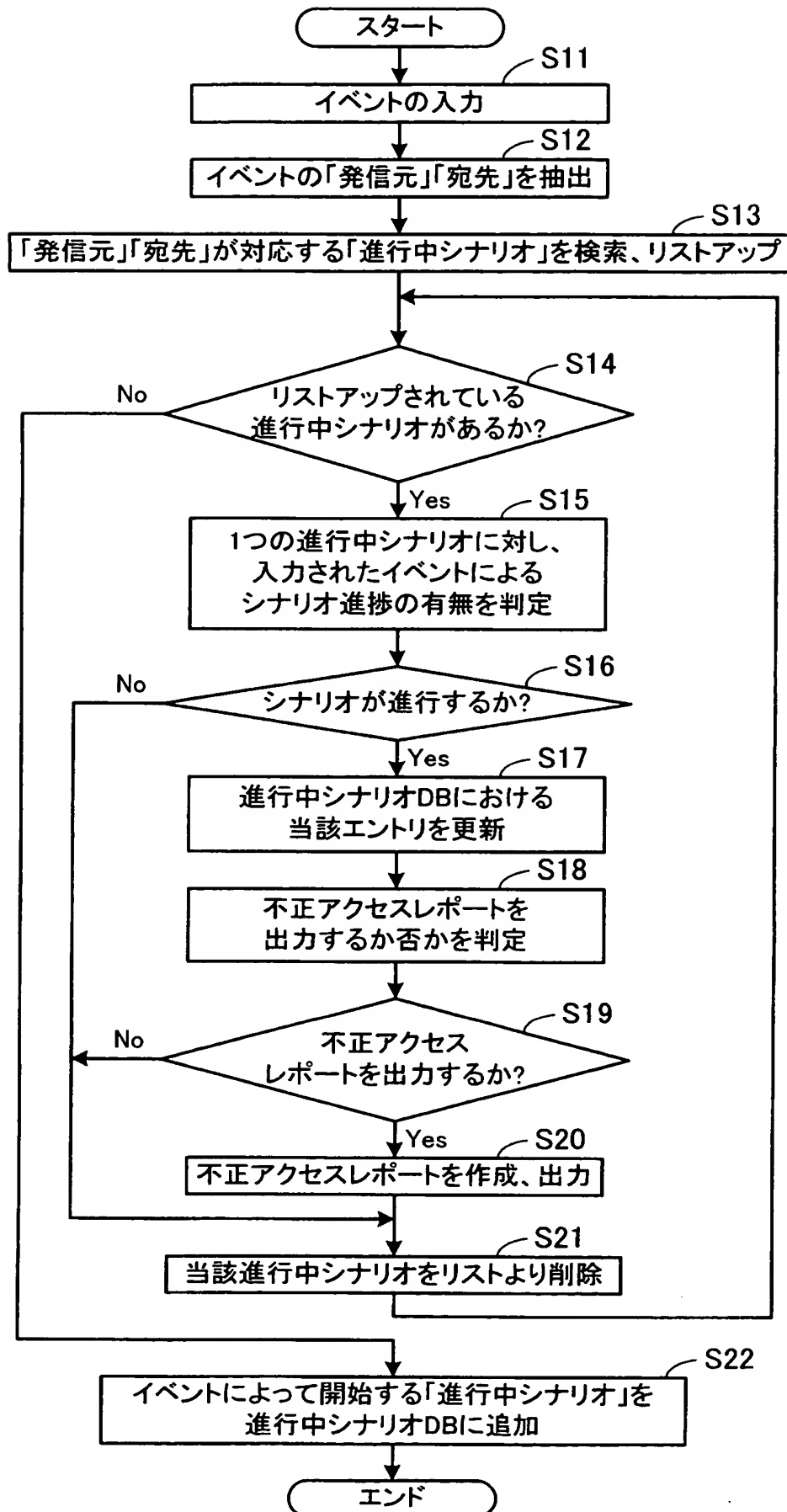
不正アクセスシナリオ名	イベント遷移
不正アクセスシナリオA	
不正アクセスシナリオB	
...	...

【図 7】

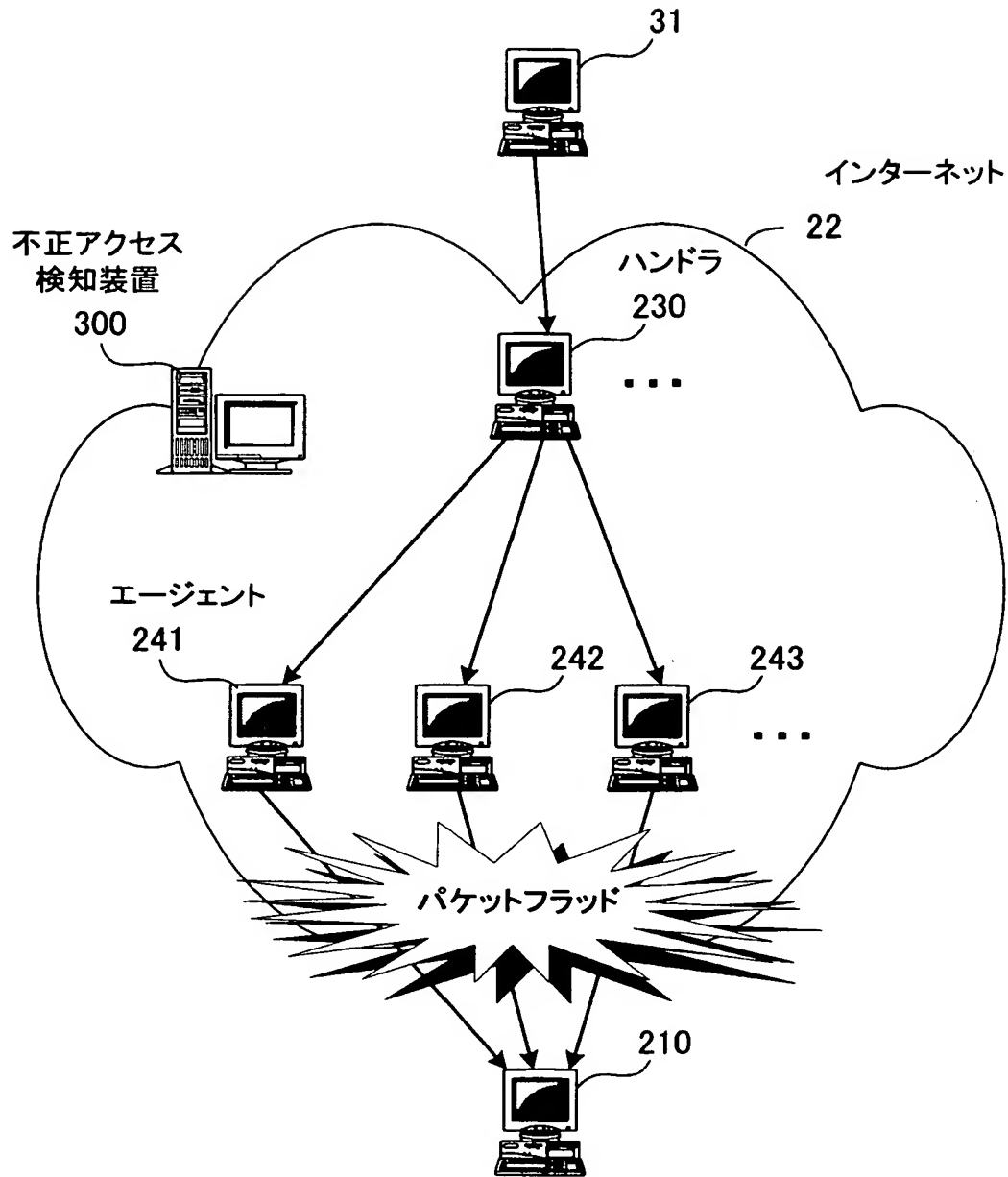
132 進行中シナリオDB

発信元IPアドレスと宛先IPアドレスとの組	不正アクセスシナリオ名	進捗度
192.168.1.5→10.10.100.100	不正アクセスシナリオB	2 番 目
10.1.1.123→192.168.30.30	不正アクセスシナリオD	3 番 目
・ ・ ・	・ ・ ・	・ ・ ・

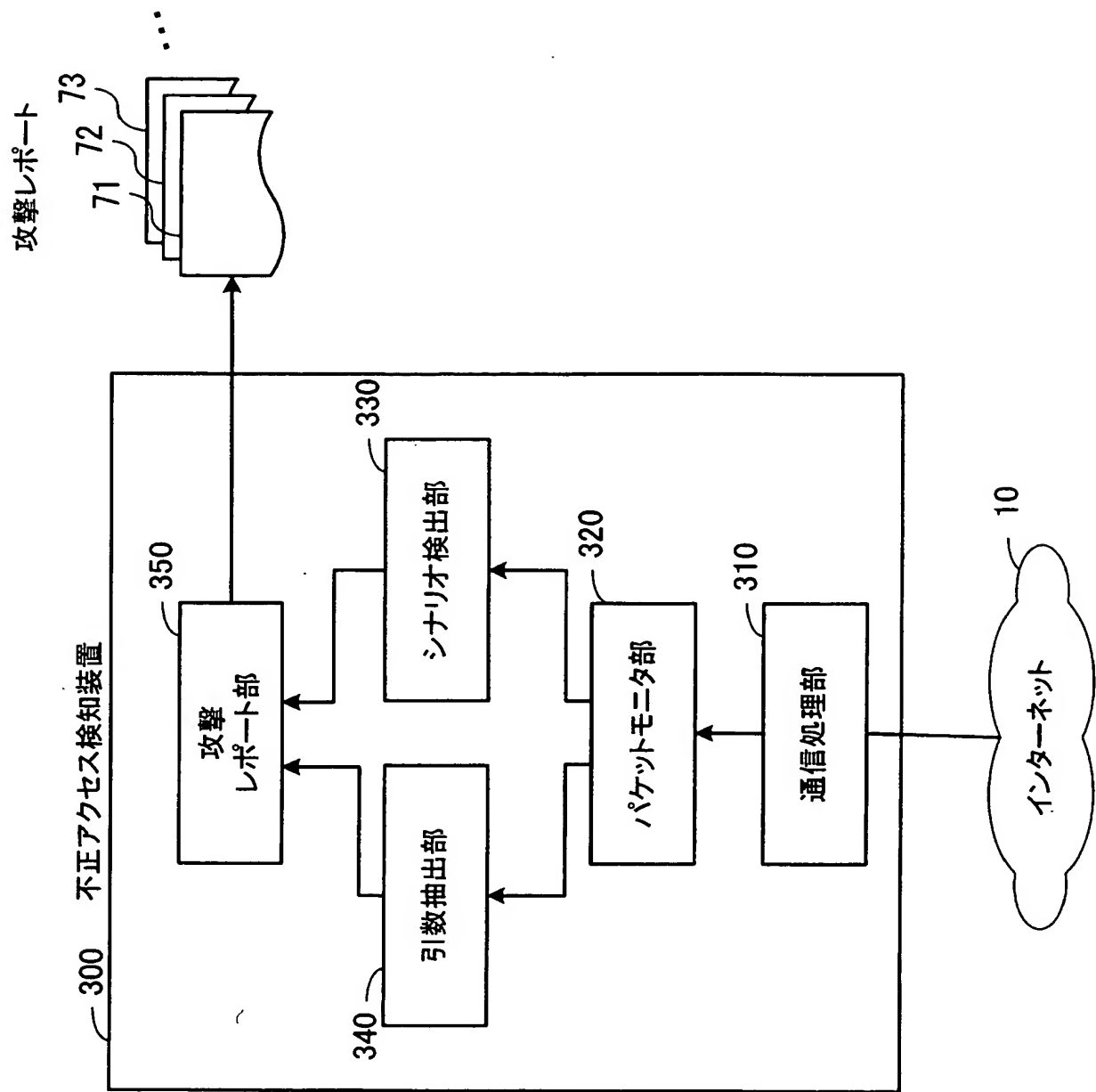
【図 8】



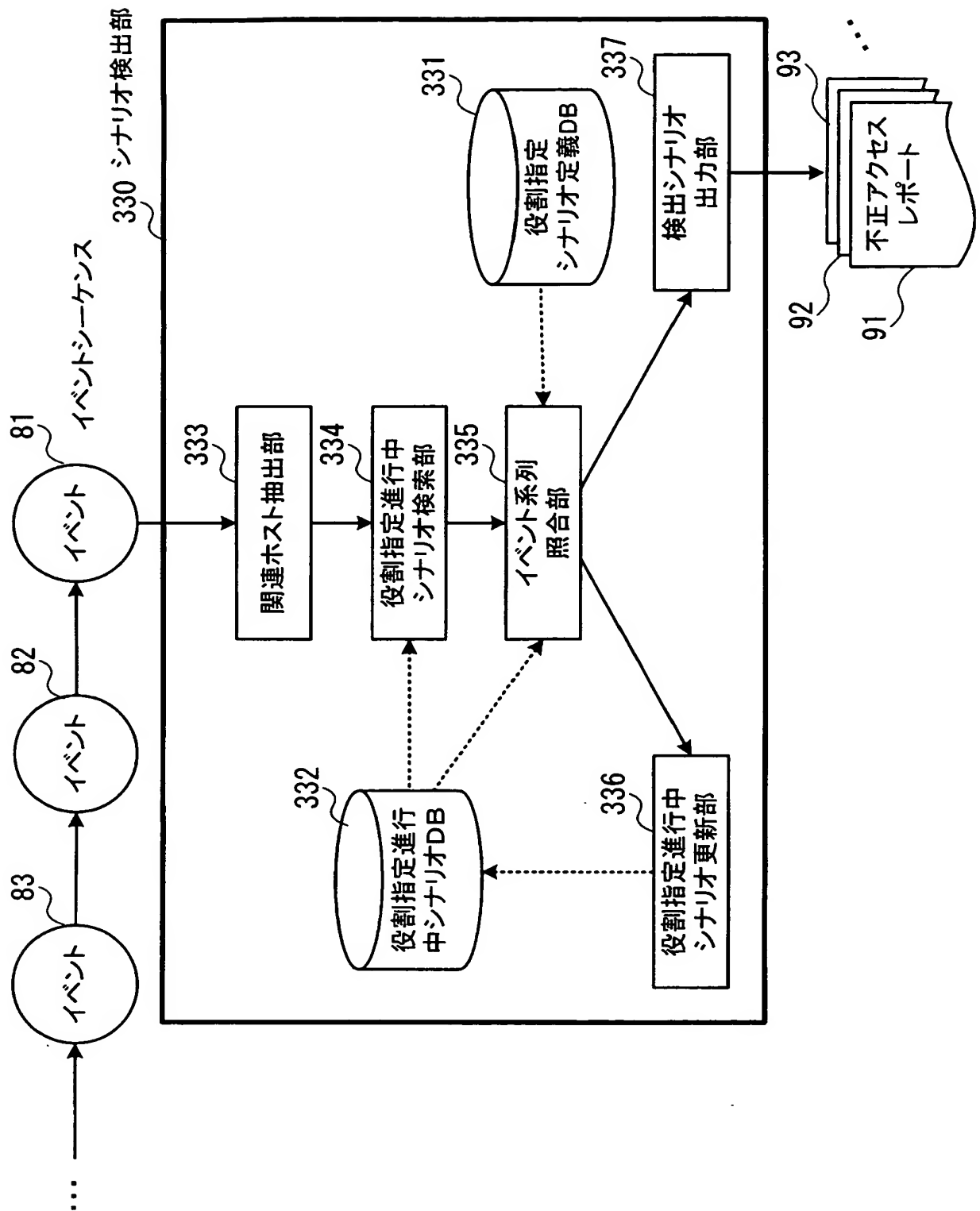
【図 9】



【図 10】

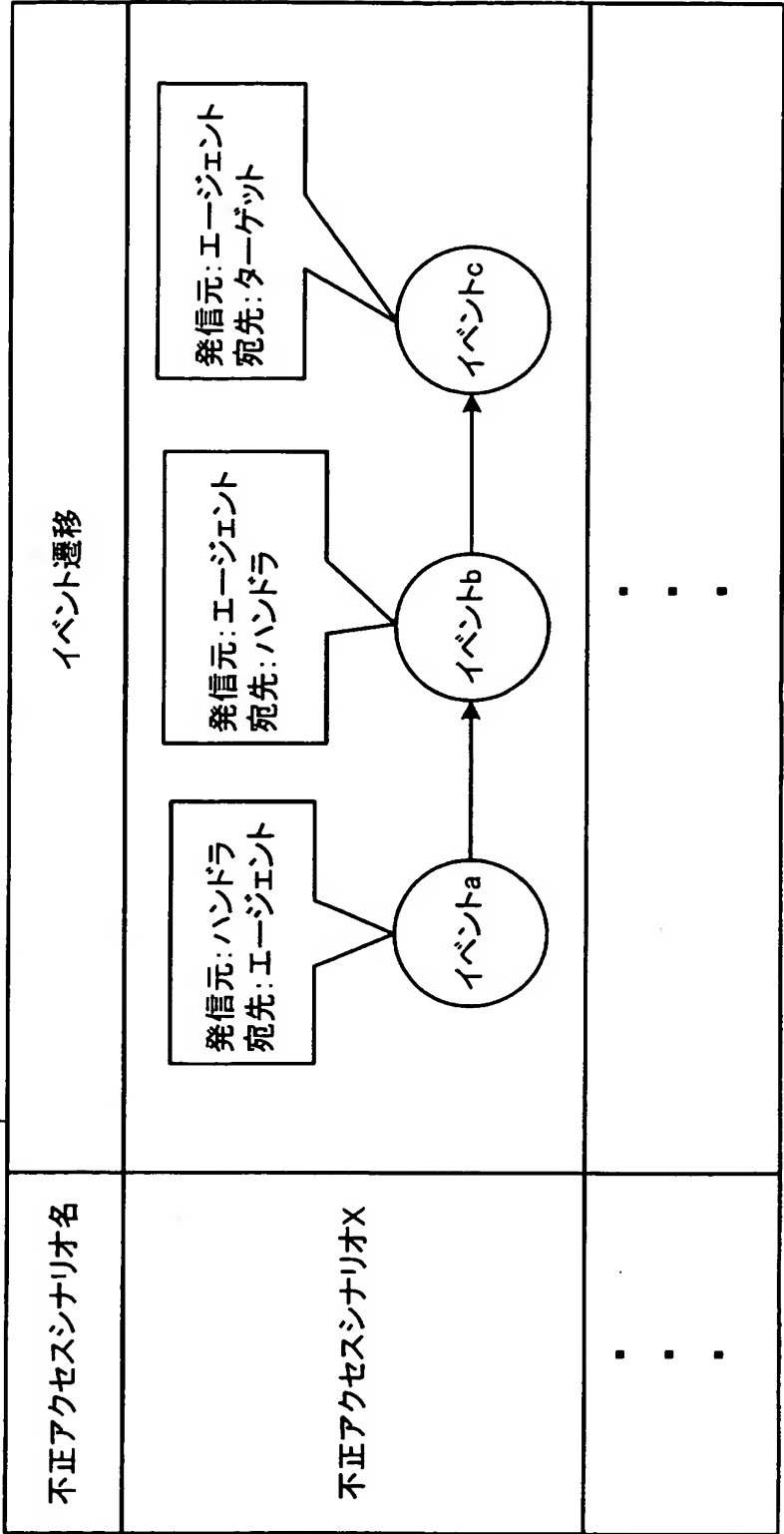


【図 11】



【図 12】

331 役割指定シナリオ定義DB

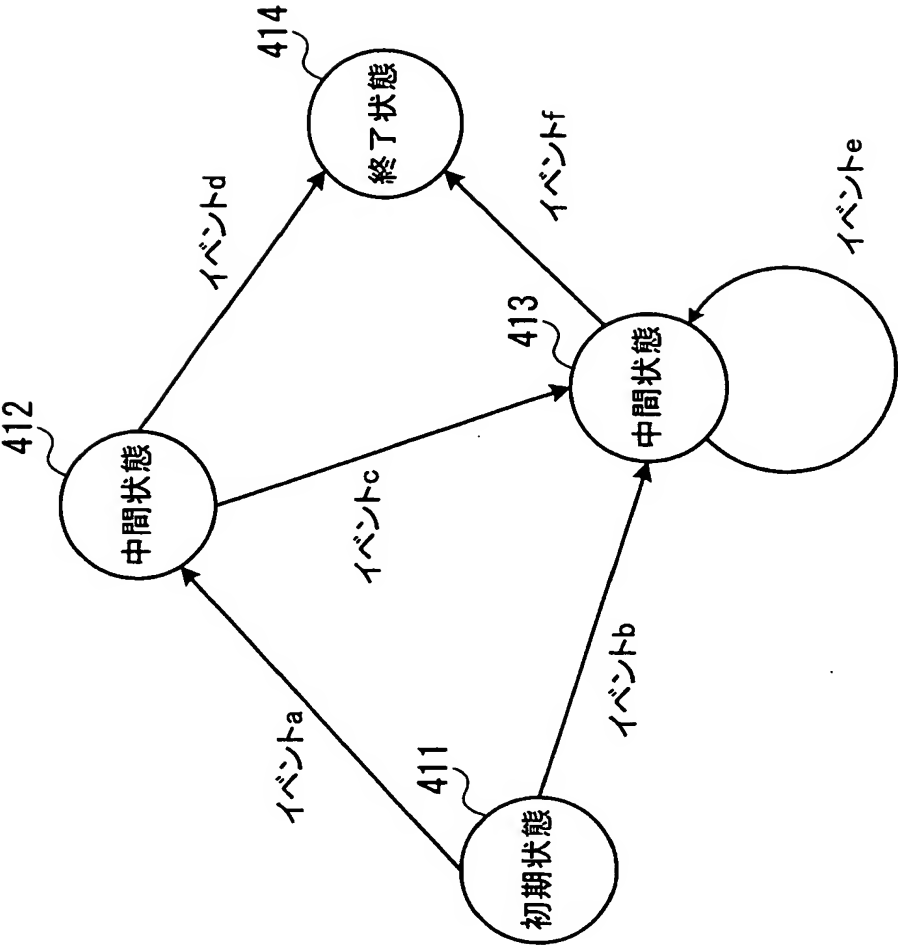


【図 1 3】

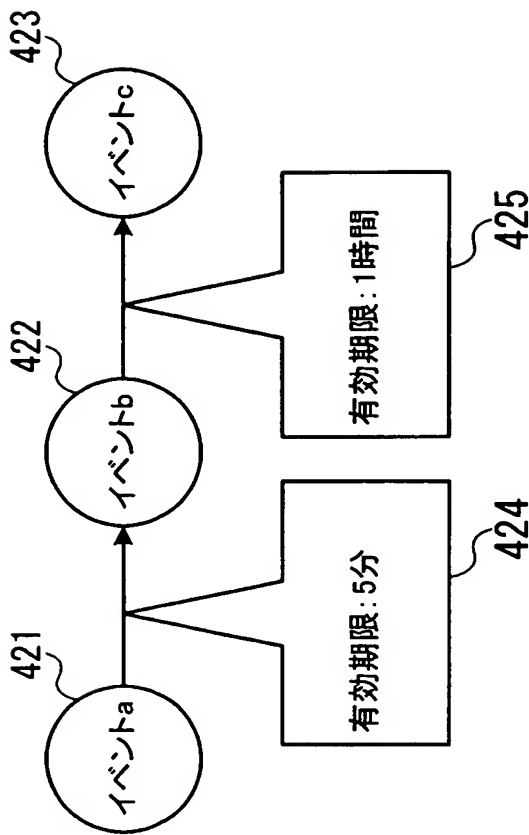
332 役割指定進行中シナリオDB

役割担当IPアドレス		不正アクセスシナリオ名	進捗度
192.168.1.5	エージェント	不正アクセスシナリオB	2 番 目
10.10.100.100	ハンドラ		
10.1.1.123	アタッカ	不正アクセスシナリオD	3 番 目
192.168.30.30	ターゲット		
・		・	・
・		・	・
・		・	・
・		・	・

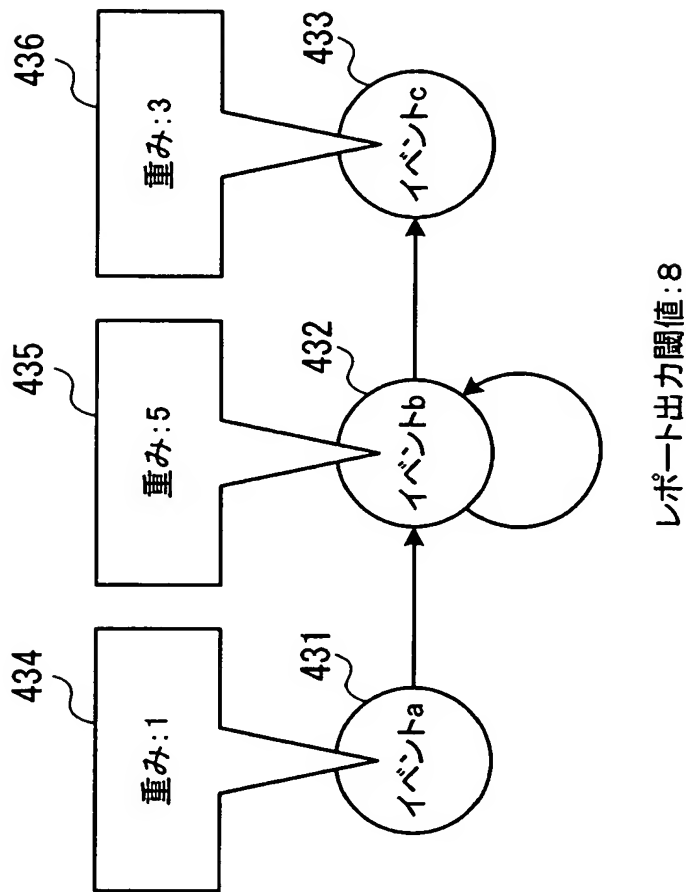
【図 14】



【図 1 5】



【図 16】

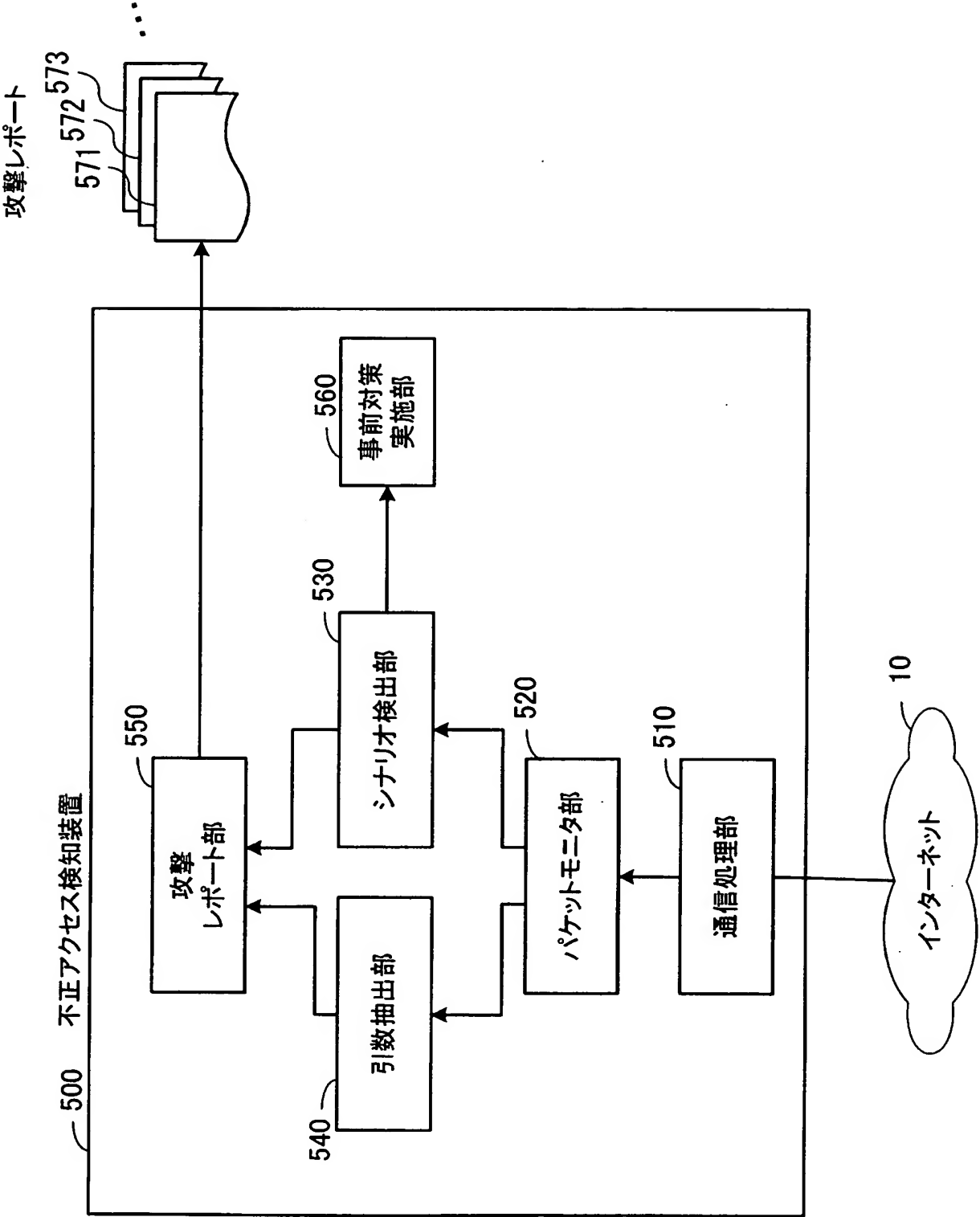


【図 1 7】

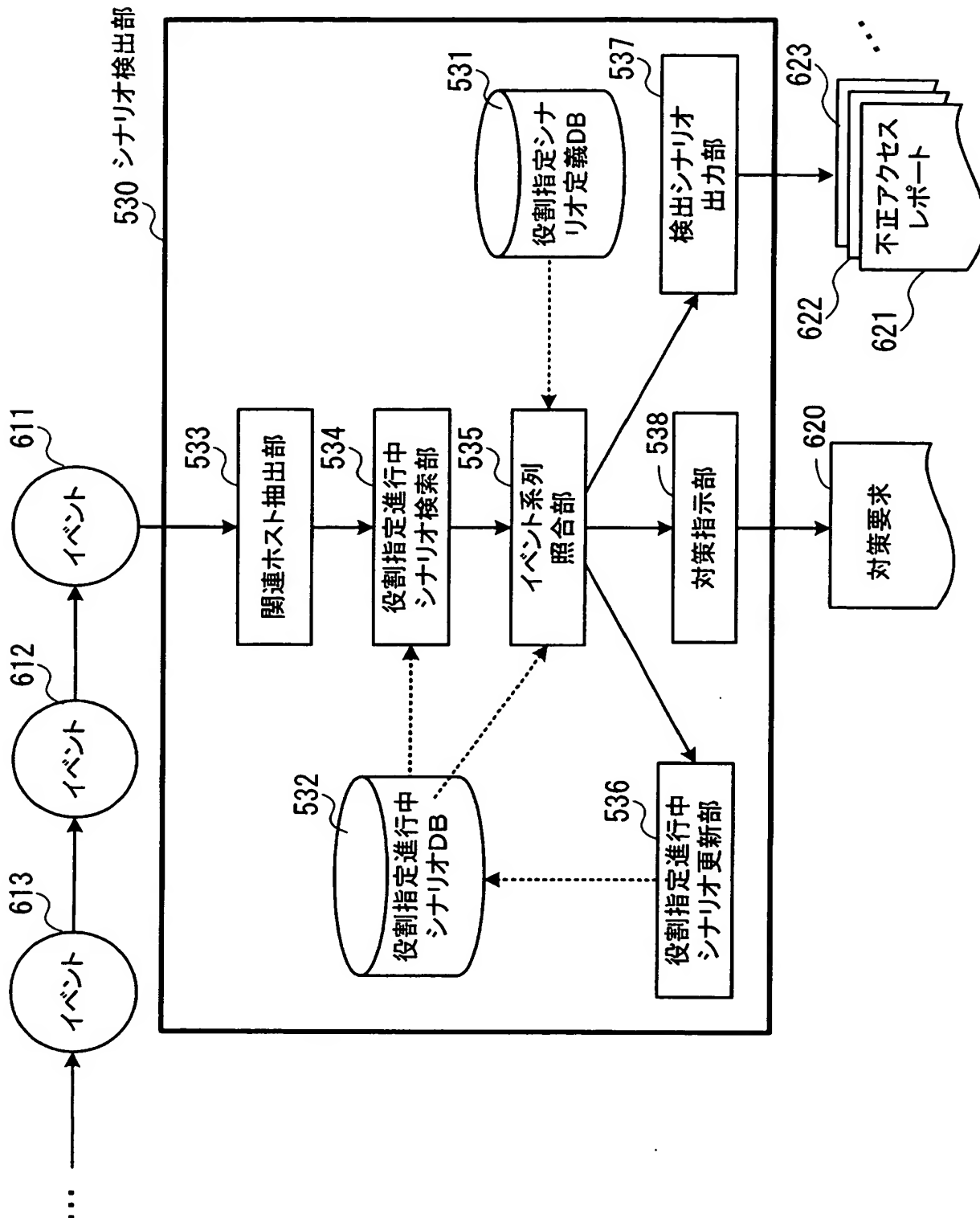
132a 進行中シナリオDB

発信元IPアドレスと宛先IPアドレスとの組	不正アクセスシナリオ名	重みトータル
192.168.1.5→10.10.100.100	不正アクセスシナリオB	6
10.1.1.123→192.168.30.30	不正アクセスシナリオD	1
・	・	・
・	・	・
・	・	・

【図 18】



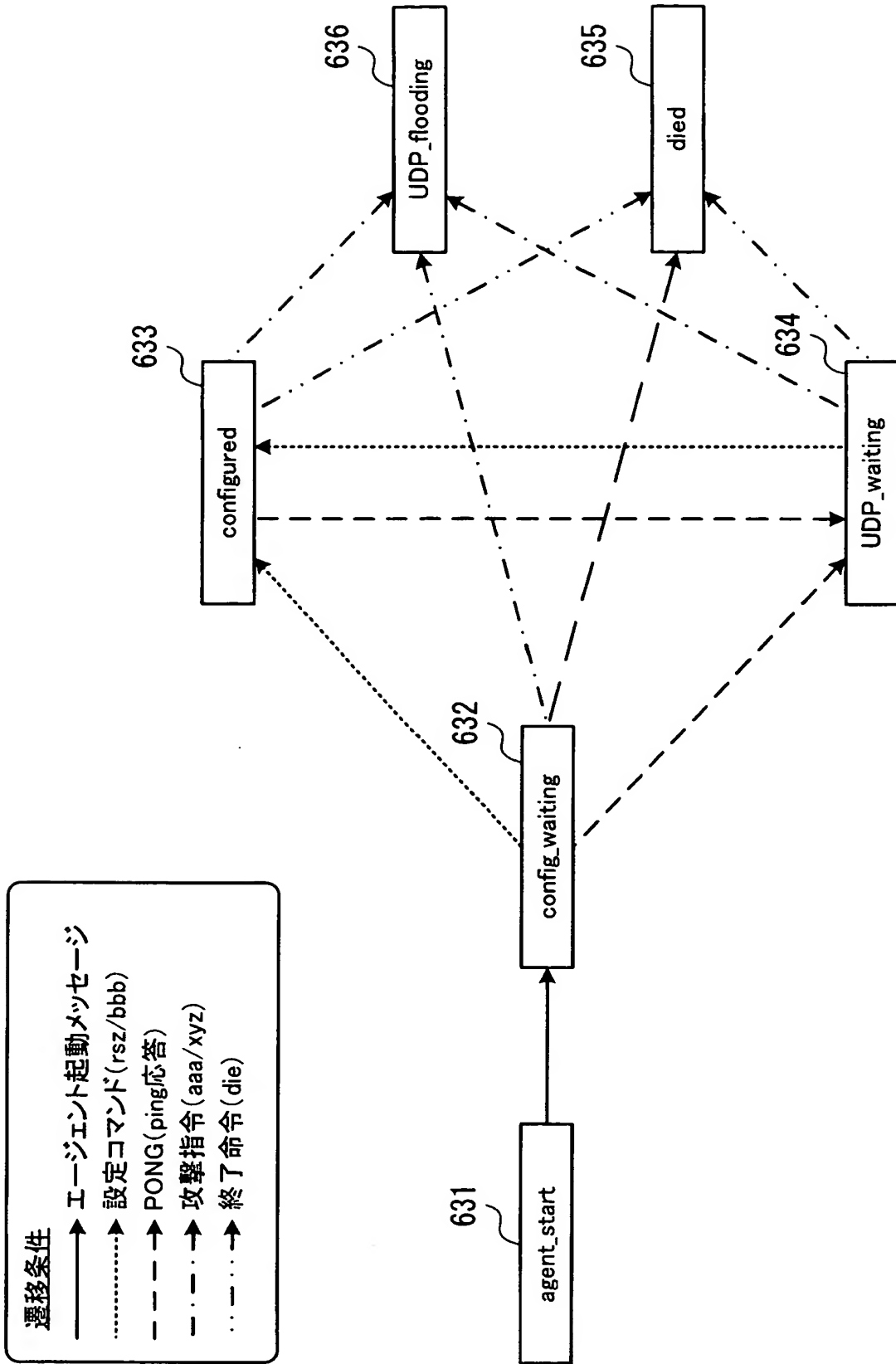
【図 19】



【図 2 0】

ハンドラ向けコマンド	エージェント向けコマンド	説明
msize	rsz	将来発生させるフラッド中の、UDPパケットのサイズ(Byte)を引数で設定
mtimer	bbb	将来発生させるフラッドの長さ(秒)を引数で設定
mping	png	全てのエージェントの生死確認
die	d1e	全てのエージェントを停止する
dos	aaa	引数指定したIPアドレスにUDPフラッドを発信
mdos	xyz	引数指定したIPアドレスにUDPフラッドを発信。複数のIPアドレスを指定できる

【図 21】



【図 2 2】

640 予測インパクト／対策定義テーブル



インパクトまでの時間	インパクトの発生確率	インパクトの大きさ	実施する対策
5分以内	70%	大	(緊急であり、インパクトも大きい為) 当該通信を、以後1時間遮断する。
1時間以内	10%	大	
1日以内	10%	中	

【図 2 3】

650 予測インパクト／対策定義テーブル

インパクトまでの時間	インパクトの発生確率	インパクトの大きさ	実施する対策
1時間以内	10%	中	(比較的時間の余裕があるため) 攻撃を起こしそうなホストの管理者(管理ホスト) に連絡する。かつ、当該通信を、以後3日間監視 し、必要に応じて遮断する。
1日以内	40%	大	
3日以内	30%	大	

【書類名】 要約書**【要約】**

【課題】 一連の処理を経て実行される不正アクセスをリアルタイムに検知することができるようにする。

【解決手段】 パケット 5 がネットワーク 2 上で通信されると、そのパケット 5 がキーデータ抽出手段 1 c で取得され、キーデータが抽出される。次に、進行中シナリオ検索手段 1 d により、キーデータ抽出手段 1 c が抽出したキーデータを検索キーとして、進行中シナリオ記憶手段 1 b から進行中シナリオが検索される。さらに、照合手段 1 e により、進行中シナリオ検索手段 1 d で検出された進行中シナリオに続けてパケット 5 で示される処理を行うことが、不正アクセスシナリオ記憶手段 1 a に格納されている不正アクセスシナリオに沿っているかどうか照合される。そして、レポート出力手段 1 g により、照合手段 1 e による照合の結果に基づいて、不正アクセスレポート 6 が出力される。

【選択図】 図 1

特願 2 0 0 3 - 3 6 8 0 6 3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 2 2 3]

1. 変更年月日 1 9 9 6 年 3 月 2 6 日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
氏 名 富士通株式会社